

# ELLIPTIC CURVES WITH FULL 2-TORSION AND MAXIMAL ADELIC GALOIS REPRESENTATIONS

DAVID CORWIN, TONY FENG, ZANE KUN LI, SARAH TREBAT-LEDER

**ABSTRACT.** In 1972, Serre showed that the adelic Galois representation associated to a non-CM elliptic curve over a number field has open image in  $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ . In [Gre10], Greicius develops necessary and sufficient criteria for determining when this representation is actually surjective and exhibits such an example. However, verifying these criteria turns out to be difficult in practice; Greicius describes tests for them that apply only to semistable elliptic curves over a specific class of cubic number fields. In this paper, we extend Greicius' methods in several directions. First, we consider the analogous problem for elliptic curves with full 2-torsion. Following Greicius, we obtain necessary and sufficient conditions for the associated adelic representation to be maximal and also develop a battery of computationally effective tests that can be used to verify these conditions. We are able to use our tests to construct an infinite family of curves over  $\mathbb{Q}(\alpha)$  with maximal image, where  $\alpha$  is the real root of  $x^3 + x + 1$ . Next, we extend Greicius' tests to more general settings, such as non-semistable elliptic curves over arbitrary cubic number fields. Finally, we give a general discussion concerning such problems for arbitrary torsion subgroups.

## 1. INTRODUCTION AND STATEMENT OF RESULTS

Let  $E$  be an elliptic curve over a number field  $K$ . For  $m$  a positive integer, let  $E[m]$  denote the group of  $m$ -torsion points of  $E$  over  $\overline{K}$ . It is well known that  $E[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ , and since  $[m]$  is defined over  $K$  the Galois group  $G_K := \mathrm{Gal}(\overline{K}/K)$  acts on  $E[m]$ . This can be phrased as a Galois representation

$$\rho_{E,m} : G_K \rightarrow \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

We call this the “mod  $m$ ” Galois representation. Now fix a prime  $\ell$ . Taking the inverse limit over powers of  $\ell$ , we obtain the *Tate module* of  $E$ ,

$$T_\ell(E) := \varprojlim \mathbb{Z}/\ell^n \mathbb{Z}$$

Correspondingly, we have the “ $\ell$ -adic” Galois representation

$$\rho_{E,\ell^\infty} : G_K \rightarrow \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Taking the product of these over all primes, we finally obtain the “adelic” Galois representation

$$\rho_E : G_K \rightarrow \mathrm{GL}_2(\widehat{\mathbb{Z}}).$$

In [Ser72], Serre famously proved that for elliptic curves *without* complex multiplication, the image of  $\rho_E$  is always open in  $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ . In particular, this implies that  $\rho_{E,\ell^\infty}$  is surjective for all sufficiently large  $\ell$ . He also showed that for an elliptic curve defined over  $\mathbb{Q}$ ,  $\rho_E$  is *never* surjective.

Naturally, this raised the question of whether  $\rho_E$  could be surjective for elliptic curves defined over number fields other than  $\mathbb{Q}$ . In [Gre10], Greicius proves necessary and sufficient abstract criteria for  $\rho_E(G_K)$  to be the full group  $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ . He then develops numerical tests applying to semistable elliptic curves over the field  $\mathbb{Q}(\alpha)$ , where  $\alpha$  is the real root of  $x^3 + x + 1 = 0$ , which can be effectively used to verify these criteria. Through the tests he is able to give the first explicit example of an elliptic curve over a number field with surjective adelic Galois representation. In doing so, the main challenge is to show that the  $\ell$ -adic representation is surjective for all  $\ell$ .

Despite the difficulty of finding explicit examples of surjective adelic representations, it turns out that much is known on average. Zywinia, building on work of Duke and Jones in [Duk97] and

[Jon10], proved that almost all (in the sense of density) elliptic curves have surjective adelic Galois representation ([Zyw10a, Zyw10b]). In fact, his work shows that for any rational family of elliptic curves, even when there are obstructions to the surjectivity of  $\rho_E$  such as the presence of torsion defined over  $K$ , the generic member has maximal Galois representation. However, his methods are ineffective in that they do not explicitly produce any such elliptic curves.

In this paper, we first consider the question of determining the image of Galois for explicit elliptic curves under certain hypotheses of torsion. More specifically, let  $E/K$  be an elliptic curve with *full* 2-torsion over  $K$ , so that  $E[2](K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . Then the action of  $G_K$  on  $E[2]$  is trivial, so the image of the 2-adic Galois representation

$$\rho_{E,2^\infty}: G_K \rightarrow \mathrm{GL}_2(\mathbb{Z}_2)$$

lies in the kernel of the reduction mod 2 map. In this case the adelic Galois representation clearly cannot be surjective. Writing  $V_k(\ell) = I + \ell^k \mathrm{Mat}_{2 \times 2}(\mathbb{Z}_\ell)$ , the remarks above imply that  $\rho_E$  factors through the map

$$\rho_E: G_K \rightarrow V_1(2) \times \prod_{\ell > 2} \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Following Greicius, we first prove necessary and sufficient abstract criteria, analogous to Theorem 3.1 in [Gre10], for the adelic Galois representation to be maximal given that the elliptic curve has full two-torsion over its field of definition,  $K$ .

**Theorem 1.1.** *Let  $K$  be a number field. We have that  $\rho_E$  surjects onto  $V_1(2) \times \prod_{\ell > 2} \mathrm{GL}_2(\mathbb{Z}_\ell)$  if and only if the following three conditions are satisfied:*

- (1)  $\rho_{E,\ell^\infty}$  is surjective for each  $\ell \geq 3$  and  $\rho_{E,2^\infty}$  surjects onto  $V_1(2)$ ,
- (2)  $K(E[4]) \cap K^{\mathrm{cyc}} = K(i)$ ,
- (3)  $K \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$ .

*Remark.* Note that the third condition cannot be satisfied when  $K$  is an abelian extension of  $\mathbb{Q}$ , so the simplest number field  $K$  where this can be satisfied is a non-Galois cubic extensions.

This theorem is not hard to prove; it is more difficult to test algorithmically if the first two conditions above are satisfied. In the case where  $K$  is the number field that Greicius considers, the first condition can be checked using his methods for most  $\ell$ , but the case of the 2-adic representation is significantly different, as there is no  $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ -module structure on the image. In Section 2.3, we develop new methods for handling this case. The second condition is also unique to the two-torsion case, and requires some work to obtain a feasible computation. Using the tests developed by Greicius, as well as the ones mentioned above, we implemented a computer program to check maximality of adelic representations. Simply iterating through coefficients, we found the following curve which has maximal adelic image.

**Example 1.2.** *Let  $K = \mathbb{Q}(\alpha)$ , where  $\alpha$  is the real root of  $x^3 + x + 1$ . Let*

$$E/K: y^2 = x(x - (2\alpha^2 + 7\alpha + 19))(x - (18\alpha^2 + 7\alpha + 3)).$$

*Then  $\rho_E$  surjects onto  $V_1(2) \times \prod_{\ell > 2} \mathrm{GL}_2(\mathbb{Z}_\ell)$ .*

Not only can our tests be used to check that specific elliptic curves have maximal adelic Galois representation, they can also be used to explicitly construct infinite families of such curves. This is done in Section 3, and we obtain the following result.

**Theorem 1.3.** *Let  $K = \mathbb{Q}(\alpha)$ , with  $\alpha$  as above. Let  $M := 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 29 \cdot 31 \cdot 47 \cdot 787 \cdot 827$  and*

$$E_{b,c}/K: y^2 = x(x - (\alpha^2 + b\alpha + c))(x - 16(\alpha^2 + \alpha + 1)).$$

If  $b, c \in \mathbb{Z}$  satisfy

$$\begin{aligned} b &\equiv 17 \cdot 37 \cdot 257 \cdot 509^2 \cdot 787 \cdot 827 \pmod{M} \\ c &\equiv 2^4 \cdot 17 \cdot 787 \cdot 827 \cdot 4657 \cdot 15649 \pmod{M}, \end{aligned}$$

then the adelic representation  $\rho_{E_{b,c}}$  surjects onto  $V_1(2) \times \prod_{\ell > 2} \mathrm{GL}_2(\mathbb{Z}_\ell)$ .

As mentioned, Greicius's tests depend upon special properties of the  $E$  and  $K$ : they apply only to semistable elliptic curves with non-integral  $j$ -invariant, and also only to cubic fields  $K$  with trivial narrow class group and possessing a totally positive unit  $u$  such that  $u - 1$  is also a unit. More precisely, Greicius uses these conditions to prove that all primes  $\ell$  failing condition 1 of Theorem 1.1, outside an easily computable finite set, satisfy a certain divisibility condition relating to the reduction of  $E$  at primes of good reduction. In Section 4, we prove analogous results applying to all elliptic curves with non-integral  $j$ -invariant over arbitrary cubic number fields.

Using them, we obtain the following examples. First, we give an example of a non-Galois cubic field  $K$  and an elliptic curve  $E/K$  with full 2-torsion over  $K$  which has maximal adelic Galois image, but is not semistable.

**Example 1.4.** Let  $\beta$  be the unique real root of  $x^3 + 4x^2 + 7x - 4$  and  $K = \mathbb{Q}(\beta)$ . The adelic representation  $\rho_E$  associated to the elliptic curve

$$E/K: y^2 = x(x + (10\beta^2 - 3))(x - (\beta + 4))$$

surjects onto  $V_1(2) \times \prod_{\ell > 2} \mathrm{GL}_2(\mathbb{Z}_\ell)$ .

Lastly, we give an example of non-galois cubic field  $K$  with nontrivial narrow class group and a semistable elliptic curve  $E/K$  with surjective adelic representation.

**Example 1.5.** Let  $\beta$  be the unique real root of  $x^3 + 8x^2 - 3x + 1$  and  $K = \mathbb{Q}(\beta)$ . Then the adelic representation  $\rho_E$  corresponding to

$$E/K: y^2 + xy + \beta y = x^3 - 8x^2 - 6x - 1$$

surjects onto  $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ .

While we focus on two-torsion in the paper, our tests may be easily generalized to higher torsion. In the final section, we discuss how to compute the  $\ell$ -adic image in the presence of  $\ell$ -torsion. As a demonstration, we compute the 7-adic Galois representation for an elliptic curve over  $\mathbb{Q}$  with a single cycle of 7-torsion points over  $\mathbb{Q}$ . In this case, the maximum possible image of Galois is the pre-image of the “half-Borel” subgroup

$$\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \subset \mathrm{GL}_2(\mathbb{F}_7)$$

under the projection  $GL_2(\widehat{\mathbb{Z}}) \rightarrow \mathrm{GL}_2(\mathbb{F}_7)$ .

**Example 1.6.** Let

$$E/\mathbb{Q}: y^2 + xy + y = x^3 - x^2 - 19353x + 958713,$$

which has torsion subgroup  $\mathbb{Z}/7\mathbb{Z}$  over  $\mathbb{Q}$ . Then  $E$  has maximal adelic image.

The computations in this paper were done using MAGMA and SAGE. Throughout this paper, we include references to the code that we have written. We indicate this by using the `typewriter` font. These scripts along with their outputs are available at [CFLT].

## 2. THE CRITERIA

We begin with the proof of Theorem 1.1.

**2.1. Proof of Theorem 1.1.** Throughout, we will assume that our elliptic curves have full 2-torsion over  $K$ , i.e., the mod 2 image of the representation is trivial. As mentioned in the introduction,

$$\rho_E(G_K) \subset V_1(2) \times \prod_{\ell > 2} \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Let

$$G := V_1(2) \times \prod_{\ell > 2} \mathrm{GL}_2(\mathbb{Z}_\ell).$$

In this section we develop a criterion for proving that the Galois representation of an elliptic curve with full 2-torsion surjects onto  $G$ .

Our approach is modeled on that in [Gre10], in which the author proves a criterion for an elliptic curve to have surjective adelic Galois representation and then uses it to compute the first known example of such a curve. To do so, he first develops a fairly abstract criterion for a subgroup of a product of profinite groups to be the whole group, and then interprets it in the case of a Galois representation associated to an elliptic curve. We summarize this result in the following lemma.

**Lemma 2.1** ([Gre10], Lemma 2.2 and Proposition 2.5). *Let  $G_\alpha$  be a collection of profinite groups such that for  $\alpha \neq \alpha'$ , we have  $\mathrm{Quo}(G_\alpha) \cap \mathrm{Quo}(G_{\alpha'}) = \emptyset$ , where  $\mathrm{Quo}(G_\alpha)$  denotes the set of isomorphism classes of finite, nonabelian simple quotients of  $G_\alpha$ . If  $H \subseteq G = \prod_\alpha G_\alpha$  is a closed subgroup that surjects onto each  $G_\alpha$  and surjects onto  $G^{\mathrm{ab}}$ , then  $H = G$ .*

Applying this to our situation, we know that

$$\rho_E(G_K) \subseteq V_1(2) \times \prod_{\ell > 2} \mathrm{GL}_2(\mathbb{Z}_\ell)$$

is a closed subgroup. The condition on  $\mathrm{Quo}(G_\alpha)$  is easily satisfied; we are in the same situation as Corollary 2.7 of [Gre10], except now we have replaced  $\mathrm{GL}_2(\mathbb{Z}_2)$  with  $V_1(2)$ . In fact,  $\mathrm{Quo}(V_1(2)) = \emptyset$ , as  $V_1(2)$  is a pro-2 group, so the condition is still satisfied. Therefore, in order to show that  $\rho_E(G_K)$  is the entire group, we must show the  $\rho_{E,\ell^\infty}$  is surjective for  $\ell \neq 2$ , that  $\rho_E(G_K)$  surjects onto  $V_1(2)$ , and that  $\rho_E(G_K)$  surjects onto the abelianization of  $V_1(2) \times \prod_{\ell > 2} \mathrm{GL}_2(\mathbb{Z}_\ell)$ .

In order to check the first two conditions, we apply the following two lemmas which are known as the Refinement Lemmas.

**Lemma 2.2** ([LT76], p. 47). *Let  $U \subseteq V_1(\ell)$  be a closed subgroup. Then the following are true.*

- (1) *If  $\ell = 2$  and  $U$  surjects onto  $V_1(\ell)/V_3(\ell)$ , then  $U = V_1(\ell)$ .*
- (2) *If  $\ell$  is odd, and  $U$  surjects onto  $V_1(\ell)/V_2(\ell)$ , then  $U = V_\ell$ .*

**Lemma 2.3** ([Ser98], IV-23). *Let  $\ell \geq 5$ . Suppose  $H \subseteq \mathrm{SL}_2(\mathbb{Z}_\ell)$  is a closed subgroup that surjects onto  $\mathrm{SL}_2(\mathbb{F}_\ell)$ . Then  $H = \mathrm{SL}_2(\mathbb{Z}_\ell)$ .*

**Corollary 2.4.** *Suppose that  $K \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$ , and suppose the following conditions are satisfied:*

- (1)  *$\rho_{E,2^\infty}(G_K)$  surjects onto  $V_1(2)/V_3(2)$ .*
- (2)  *$\rho_{E,9}(G_K)$  is surjective.*
- (3)  *$\rho_{E,\ell}(G_K)$  is surjective for all  $\ell > 3$ .*

*Then  $\rho_{E,2^\infty}$  surjects onto  $V_1(2)$ , and  $\rho_{E,\ell^\infty}$  is surjective for all odd  $\ell$ .*

*Proof.* The surjectivity for the 2-adic and 3-adic representations follows from the two parts of Lemma 2.2, respectively.

Furthermore, if we assume that  $K \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$ , then, by the non-degeneracy of the Weil pairing, the determinant map is surjective. The hypothesis in our corollary implies that  $\rho_{E,\ell}(G_K)$  contains  $\mathrm{SL}_2(\mathbb{F}_\ell)$ , so  $\rho_{E,\ell^\infty}(G_K)$  contains  $\mathrm{SL}_2(\mathbb{Z}_\ell)$ . As the determinant is surjective, this implies that  $\rho_{E,\ell^\infty}$  is surjective.  $\square$

In order to show that  $\rho_E(G_K)$  surjects onto the abelianization, we must compute the abelianization of  $V_1(2) \times \prod_{\ell > 2} \mathrm{GL}_2(\mathbb{Z}_\ell)$ . Equivalently, we wish to compute its commutator subgroup. We note that we only need to do this for each  $\ell$  separately. For any group  $G$ , we denote the commutator subgroup of  $G$  by  $G'$ . We recall the computation for  $\ell$  odd.

**Lemma 2.5** ([LT76], p. 95 and 183). *Let  $\ell$  be odd. Then  $\mathrm{GL}_2(\mathbb{Z}_\ell)' = \mathrm{SL}_2(\mathbb{Z}_\ell)$ .*

The only task then is to compute  $V_1(2)'$ .

**Lemma 2.6.** *We have  $V_1(2)' = V_2(2) \cap \mathrm{SL}_2(\mathbb{Z}_2)$ .*

*Proof.* As  $V_1(2)/V_2(2)$  is abelian, we know the commutator is contained in  $V_2(2)$ . As usual, we know that  $\mathrm{SL}_2(\mathbb{Z}_2)$  contains the commutator, so we have an inclusion above in one direction. We write  $U_k(\ell) = V_k(\ell) \cap \mathrm{SL}_2(\mathbb{Z}_\ell)$ .

First, we would like to show that modulo 8, the image of  $V_1(2)'$  contains  $U_2(2)$ . In other words, we would like to compute the commutator of  $V_1(2)/V_3(2)$ .

We note that

$$\left[ \begin{pmatrix} 3 & 0 \\ 2 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 2 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix} \quad \text{and} \quad \left[ \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & 4 \\ 4 & 1 \end{pmatrix}.$$

Transposing the first, we get the matrix  $\begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}$ . These three matrices generate  $U_2(2)/U_3(2)$ , so we know that this is the commutator of  $V_1(2)/V_3(2)$ , and this means that  $V_1(2)'$  surjects onto  $U_2(2)/U_3(2)$ .

Suppose that  $V_1(2)'$  surjects onto  $U_{k-1}(2)/U_k(2)$ . Note that  $U_k(\ell) = I + \ell^k \mathfrak{sl}_2(\mathbb{Z}_\ell)$ , where  $\mathfrak{sl}_2$  is the set of  $2 \times 2$  matrices with trace 0. We know that  $V_1(2)'$  contains all matrices of the form  $1 + 2^{k-1}A$ , as  $A$  runs over the matrices of trace zero modulo 2. In general, if  $k \geq 2$  or  $\ell \geq 3$ , we know that  $(1 + \ell^k A)^2 \equiv 1 + \ell^{k+1}A \pmod{\ell^{k+2}}$ , and this only depends on  $A$  modulo  $\ell$ . It follows that  $V_1(2)'$  also surjects onto  $U_k(2)/U_{k+1}(2)$ . Since we know that  $V_1(2)'$  surjects onto  $U_2(2)/U_3(2)$ , we know that it surjects onto  $U_k(2)/U_{k+1}(2)$  for all  $k \geq 2$ . Thus  $V_1(2)'$  surjects onto  $U_2(2)/U_k(2)$ , and since  $V_1(2)'$  is closed, it must be all of  $U_2(2)$ .  $\square$

So we see that the abelianization map of  $G$  is the product  $\rho_{E,4} \times \det$ , and its image is the index two subgroup of  $V_2/V_4 \times \widehat{\mathbb{Z}}^*$  where  $\det$  (on the first factor) and reduction mod 2 (on the second factor) agree.

We would like to interpret surjectivity onto  $G^{\mathrm{ab}}$  in a field-theoretic manner. As we noted, showing that the determinant map is surjective is a matter of requiring that  $K \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$ . In order for  $\rho_E(G_K)$  to surject onto  $G^{\mathrm{ab}}$  in our case, we need the following:

**Proposition 2.7.** *The group  $\rho_E(G_K)$  surjects onto  $G^{\mathrm{ab}}$  if and only if  $K \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$ ,  $[K(E[4]) : K] = 16$ , and  $K(E[4]) \cap K^{\mathrm{cyc}} = K(i)$ .*

*Proof.* We have already remarked that  $K \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$  is equivalent to the surjectivity of the determinant map.

Observe that  $K(E[4])$  is the fixed field of  $\rho_{E,2^\infty}(G_K) \cap (I + 4V_1(2))$ . Furthermore,  $K(E[4]) \cap K^{\mathrm{cyc}} \supset K(i)$  by properties of the Weil pairing. The abelianization map can be restated as the product of the quotient maps from  $G_K$  to  $\mathrm{Gal}(K(E[4])/K)$  and  $\mathrm{Gal}(K^{\mathrm{cyc}}/K)$  given by restriction to the respective fields; under this interpretation, the condition is simply that the image of an element  $\sigma \in G_K$  must agree under the restriction of both factors to  $K(i)$ .

We know that if  $L$  and  $M$  are extensions of  $K$ , then  $\mathrm{Gal}(LM/K) \cong \mathrm{Gal}(L/K) \times_{\mathrm{Gal}(L \cap M)/K} \mathrm{Gal}(M/K)$ , and the result follows. Therefore, if  $K(E[4]) \cap K^{\mathrm{cyc}} = K(i)$ , then the Galois group of the compositum already surjects onto  $G^{\mathrm{ab}}$ . Conversely, if the intersection is any greater, then the map cannot be surjective because its image is constrained to agree on the Galois group of the intersection over  $K$ , which strictly contains  $K(i)$ .  $\square$

**2.2. Checking condition 2.** As the second condition of Theorem 1.1 cannot be directly computed, we must develop an easier criterion to check. Greicius does not have to do this, as his version of the second condition is that  $K(\sqrt{\Delta}) \cap K^{\text{cyc}} = K$ , so all that must be checked is if  $\sqrt{\Delta} \in K^{\text{cyc}}$ . We avoid working with  $K(E[4])$  directly, as that would be computationally intensive. Instead, we develop a test in which we only see if certain elements of  $K$  are squares.

We use the following notation. Let  $T$  be a set of numbers. Define  $\mathcal{P}_T$  to be the set containing all products of non-empty subsets of elements of  $T$ . For example, if  $T = \{2, 3\}$ , then  $\mathcal{P}_T = \{2, 3, 6\}$ . We define  $\Delta$  to be the discriminant of  $E$ .

**Proposition 2.8.** *Assume that  $[K(E[4]) : K] = 16$  and  $K \cap \mathbb{Q}^{\text{cyc}} = \mathbb{Q}$ . Let  $d_1, d_2, d_3$  be the discriminants of the three quadratic factors of the 4-division polynomial. Let  $d_4 = \sqrt{\Delta}$ . Let  $S'$  be the set of prime ideals of  $K$  dividing  $2\Delta$  and  $S$  be the primes of  $\mathbb{Q}$  below primes in  $S'$ . Let  $T = \{d_1, d_2, d_3, d_4\}$ . If  $K(E[4]) \cap K^{\text{cyc}} \supsetneq K(i)$ , then there exists  $s \in \mathcal{P}_S, t \in \mathcal{P}_T$  such that  $t/s$  is a square in  $K$ .*

*Proof.* From p. 81-82 of [Ade01], we have that if  $E$  is in the form  $y^2 = x^3 + Ax + B$ , then  $K(E[4]) = K(x(E[4]), \sqrt[4]{\Delta}) = K(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3}, \sqrt{d_4})$ . Our curves are not of that form, but using the change of variables from pg. 41 - 43 of [Sil09], we get that the same result holds for all elliptic curves in Weierstrass form.

Assume that  $K(E[4]) \cap K^{\text{cyc}} = M' \supsetneq K(i)$ . We have that  $\text{Gal}(K(E[4])/K) \cong (\mathbb{Z}/2\mathbb{Z})^4$ , so there exists  $M$  with  $K(i) \subset M \subset M'$  and  $\text{Gal}(M/K) \cong (\mathbb{Z}/2\mathbb{Z})^2$ . The extension  $M/K$  has two quadratic subextensions in addition to  $K(i)$ . Let  $L := K(\sqrt{d})$ , where  $d \in \mathcal{O}_K$  is square-free, be one of them.

As  $L \subset K^{\text{cyc}}$ , choose  $n$  such that  $L \subset K(\mu_n)$ . Since  $K \cap \mathbb{Q}^{\text{cyc}} = \mathbb{Q}$ , we have that  $\text{Gal}(K(\mu_n)/K) \cong \text{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$ . So we may consider  $\mathbb{Q} \subsetneq L' := \mathbb{Q}(\mu_n)^{\text{Gal}(K(\mu_n)/L)} \subset \mathbb{Q}(\mu_n)$ . By the fundamental theorem of Galois theory,  $L' \subset L$ . So  $L \cap \mathbb{Q}^{\text{cyc}} \neq \mathbb{Q}$ . This implies that  $\sqrt{d} \in \mathbb{Q}^{\text{cyc}}$ , and hence  $d \in \mathbb{Q}^{\text{cyc}} \cap \mathcal{O}_K = \mathbb{Z}$ . We may assume that  $d$  is positive, as  $i \in M$ .

By the criterion of Neron-Ogg-Shafarevich, we have that a prime ideal  $\mathfrak{p} \subset \mathcal{O}_K$  ramifies in  $K(E[4])/K$  only if  $\mathfrak{p} \in S'$ . Therefore, we must have that  $d \in \mathcal{P}_S$ .

Since  $K(E[4]) = K(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3}, \sqrt{d_4})$ , we have that all quadratic subextensions of  $K(E[4])/K$  are generated by an element of  $\mathcal{P}_T$ . Therefore, we have that  $L = K(\sqrt{t})$  for some  $t \in \mathcal{P}_T$ . Now,  $K(\sqrt{t}) = K(\sqrt{s})$  if and only if  $t/s$  is a square of  $K$ , which completes the proof of our lemma.  $\square$

**2.3. 2-adic surjectivity.** We now outline our algorithm for checking that the 2-adic image is the full group  $V_1(2)$ . We assume that the 2-adic image surjects onto  $V_1(2)/V_2(2)$ ; this is easily checked by, for instance, computing the degree of the field extension  $K(E[4])/K$ . In contrast, computing directly the degree of the extension  $K(E[8])/K$  is infeasible, as we want examples where this extension has degree 256.

In what follows, let  $\mathfrak{p}$  be a prime of  $K$  not dividing  $2\Delta$ , where  $\Delta$  is the discriminant of  $E$  (so that the 2-adic Galois representation is unramified at these primes). Let  $\tilde{E}_{\mathfrak{p}}$  denote the reduction of  $E$  at  $\mathfrak{p}$ . Let  $\text{Frob}_{\mathfrak{p}}$  denote the Frobenius element at  $\mathfrak{p}$  for the extension  $\bar{K}/K$ .

**Proposition 2.9.** *Under the hypothesis above, the 2-adic Galois representation associated to  $E$  has maximal image if the following is satisfied: there exists a prime  $\mathfrak{p} \subset \mathcal{O}_K$  such that  $\#(\mathcal{O}_K/\mathfrak{p}) \equiv 5 \pmod{8}$  and  $E \pmod{\mathfrak{p}}$  has full four-torsion over  $\mathcal{O}_K/\mathfrak{p}$ .*

*Proof.* By the Refinement Lemmas ([LT76], p. 47), it suffices to show that the 2-adic image surjects onto  $V_1(2)/V_3(2)$ . Since we know that it surjects onto  $V_1(2)/V_2(2)$ , the mod 8 image contains an element of the form  $I + 2S + 4T$  for all  $2 \times 2$  matrices  $S \in \text{Mat}_{2 \times 2}(\mathbb{Z}/2\mathbb{Z})$ . Squaring, we obtain

$$(I + 2S + 4T)^2 \equiv I + 4(S + S^2) \pmod{8}.$$

Computing this for all such  $S$ , we find five distinct matrices:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}, \begin{pmatrix} 5 & 4 \\ 4 & 5 \end{pmatrix}, \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}.$$

Note that this set generates a subgroup of size 8 in  $V_2(2)/V_3(2)$  consisting of those matrices with determinant congruent to 1 (mod 8). Therefore, we immediately see that (under our hypotheses) the image of Galois, contains an index two subgroup of  $V_2(3)/V_2(3)$  and hence also  $V_1(3)/V_3(3)$ . Moreover, equality is achieved in both cases if and only if the mod 8 image of Galois has an element with determinant congruent to 5 (mod 8) in  $V_2(2)/V_3(2)$ .

Since the 8-torsion of  $E$  injects into the 8-torsion of  $\tilde{E}_{\mathfrak{p}}$ , the first condition implies that in some basis for  $E[8]$ ,

$$\rho_{E,4}(\text{Frob}_{\mathfrak{p}}) = I \implies \rho_{E,8}(\text{Frob}_{\mathfrak{p}}) \equiv I \pmod{4}$$

but has determinant congruent to 5 (mod 8).  $\square$

**2.4. Proof of Example 1.2.** In this section we apply the results of Section 2 and give an example of an elliptic curve over  $K = \mathbb{Q}(\alpha)$  with surjective adelic Galois representation  $\rho_E$ .

Let

$$E/K : y^2 = x(x - (2\alpha^2 + 7\alpha + 19))(x - (18\alpha^2 + 7\alpha + 3)).$$

We want to show that  $\rho_E$  surjects onto  $V_1(2) \times \prod_{\ell > 2} \text{GL}_2(\mathbb{Z}_{\ell})$ .

It is clear from the definition of  $E$  that  $E$  has full 2-torsion over  $K$ . As the conductor of  $E$  is squarefree,  $E$  is semistable. We now check that the three conditions of Theorem 1.1 are satisfied. Since  $K = \mathbb{Q}(\alpha)$ , it is clear that  $K \cap \mathbb{Q}^{\text{cyc}} = \mathbb{Q}$ .

As an ideal the discriminant of  $E$  is

$$(1) \quad (\Delta) = (2)^{12}(2\alpha^2 + 7\alpha + 19)^2(5\alpha^2 + \alpha + 4)^2(\alpha - 3)^2(\alpha - 1)^2$$

where the ideals on the right hand side of the above equation are prime ideals which lie above 2, 6857, 167, 31, and 3, respectively.

Using MAGMA, one can compute that  $[K(E[4]) : K] = 16$ . We now show that  $K(E[4]) \cap K^{\text{cyc}} = K(i)$ . This will make use of Lemma 2.8. To apply the theorem, we make some computational preliminaries to explicitly write out  $K(E[4])$ . Note that the division polynomial of  $E$  will factor as the product of 3 quadratic factors  $f_1$ ,  $f_2$ , and  $f_3$ . From Section 5.5 of [Ade01] and the fact that  $[K(E[4]) : K] = 16$ , we know that  $K(E[4]) = K(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3}, \sqrt[4]{\Delta})$  where  $d_i$  is the discriminant of  $f_i$ . In this case, we have

$$\begin{aligned} d_1 &= 361\alpha^2 - 22\alpha - 83 \\ d_2 &= -2112\alpha^2 - 2048\alpha - 640 \\ d_3 &= -372\alpha^2 + 1976\alpha + 1552. \end{aligned}$$

We also have that

$$d_4 := \sqrt{\Delta} = 2^6\alpha^3(2\alpha^2 + 7\alpha + 19)(18\alpha^2 + 7\alpha + 3)(\alpha - 1).$$

In the notation of Lemma 2.8, we have  $S = \{2, 3, 31, 167, 6857\}$  and  $T = \{\sqrt{d_i}\}_{i=1}^4$ . Let

$$S_1 = \{2^{r_1}3^{r_2}31^{r_3}167^{r_4}6857^{r_5} : r_i = 0 \text{ or } 1\} \setminus \{1\}$$

and

$$T_1 = \{d_1^{s_1}d_2^{s_2}d_3^{s_3}d_4^{s_4} : s_i = 0 \text{ or } 1\} \setminus \{1\}.$$

Lemma 2.8 implies that if for all possible pairs of  $\beta \in S_1$  and  $\gamma \in T_1$  if  $\gamma/\beta$  is not a square in  $K$ , then  $K(E[4]) \cap K^{\text{cyc}} = K(i)$ . Writing a script in MAGMA iterating through all 465 pairs of  $(\beta, \gamma)$  yields that this condition is indeed satisfied (see `ex12_sq.txt` and the corresponding `ex12_sq_res.txt` in [CFLTL]). Therefore we have  $K(E[4]) \cap K^{\text{cyc}} = K(i)$ .

Let  $H := \rho_E(G_K)$ . Denote by  $H_\ell$  the image of  $H$  under  $\pi_\ell : H \rightarrow \mathrm{GL}_2(\mathbb{Z}_\ell)$ , and similarly denote by  $H(\ell)$  the image of  $H$  under  $r_\ell : H \rightarrow \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ . Since  $[K(E[4]) : K] = 16$ , the mod 4 image  $H(4)$  is maximal. This and the fact that  $K(E[4]) \cap K^{\mathrm{cyc}} = K(i)$  imply that the abelianization map is surjective. We will also need this fact in proving that  $\rho_{E,2^\infty}$  is surjective.

We now verify the first condition in Theorem 1.1. That is,  $H_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$  for  $\ell \geq 3$  and  $H_2 = V_1(2)$ . The ideal generated by the  $j$ -invariant of  $E$  is

$$(j_E) = \frac{(\alpha^2 - 6\alpha + 3)^3(3\alpha^2 - 5\alpha + 1)^3(5\alpha^2 + 2\alpha + 6)^3}{(5\alpha^2 + \alpha + 4)^2(\alpha - 1)^2(\alpha - 3)^2(2\alpha^2 + 7\alpha + 19)^2}.$$

Equation (1) gives the primes of bad reduction. For all primes of bad reduction which are not the ideal (2), we have  $v(j_E) = -2$ . To show that  $H_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$  for all  $\ell \neq 2, 3, 31$ , we will make use of a combination of Proposition 3.5, Corollary 3.8, and Remark 3.9 in [Gre10] which we state below:

**Proposition 2.10.** *Let  $K$  be a number field with a real embedding and a trivial narrow class group and satisfying  $K \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$ . Let  $E/K$  be a semistable elliptic curve with  $j$ -invariant  $j_E$ . Suppose  $\ell$  is a prime unramified in  $K$ . If  $\ell = 2, 3, 5$ , suppose further that  $\ell \nmid v(j_E)$  for some  $v$  corresponding to a prime of bad reduction of  $E$ . If  $H(\ell) \neq \mathrm{GL}_2(\mathbb{F}_\ell)$ , given any place  $v'$  not of bad reduction, we have  $\ell \mid \#\tilde{E}_{v'}(k_{v'})$  where  $\tilde{E}_{v'}(k_{v'})$  is the reduction of  $E$  over the residue field corresponding to  $v'$ .*

Fix an  $\ell \neq 2, 31$ . Assume that  $H(\ell) \neq \mathrm{GL}_2(\mathbb{F}_\ell)$ . Let  $v$  be the prime ideal  $(1 - 2\alpha)$  which lies over 13. Then  $\#\tilde{E}_v(k_v) = 16$  and hence by Proposition 2.10,  $\ell \mid 16$ . Since  $\ell$  is prime, we must have  $\ell = 2$ , a contradiction. Therefore  $H(\ell) = \mathrm{GL}_2(\mathbb{F}_\ell)$  for all  $\ell \neq 2, 31$ .

We now use the following result which is a corollary of Lemma 2.3.

**Proposition 2.11** ([Gre10], Corollary 2.13 (iii)). *Let  $K \subseteq \mathrm{GL}_2(\mathbb{Z}_\ell)$  be a closed subgroup. If  $\ell \geq 5$ ,  $K \twoheadrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$  and  $\det(K) = \mathbb{Z}_\ell^*$ , then  $K = \mathrm{GL}_2(\mathbb{Z}_\ell)$ .*

For  $\ell \neq 2, 3, 31$ , the previous proposition and the surjectivity of  $\det|_H$  imply that  $H_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$  for all  $\ell \neq 2, 3, 31$ . It now remains to show the last 3 cases.

Consider the  $\ell = 31$  case. This case will make use of the following proposition.

**Proposition 2.12** ([Ser72], Proposition 19). *Let  $\ell \geq 5$  and suppose  $K \subseteq \mathrm{GL}_2(\mathbb{F}_\ell)$  is a subgroup satisfying*

- (i)  *$K$  contains elements  $s_1$  and  $s_2$  such that  $\left(\frac{\mathrm{tr}(s_i)^2 - 4\det(s_i)}{\ell}\right) = (-1)^i$  and  $\mathrm{tr}(s_i) \neq 0$ .*
- (ii)  *$K$  contains an element  $t$  such that  $u = \mathrm{tr}(t)^2/\det(t) \not\equiv 0, 1, 2, 4 \pmod{\ell}$  and  $u^2 - 3u + 1 \not\equiv 0 \pmod{\ell}$ .*

*Then  $K$  contains  $\mathrm{SL}_2(\mathbb{F}_\ell)$ . In particular, if  $\det : K \rightarrow \mathbb{F}_\ell^*$  is surjective, then  $K = \mathrm{GL}_2(\mathbb{F}_\ell)$ .*

We compute the following table. By  $t_v$  and  $N_v$ , we mean the trace of the Frobenius corresponding to  $v$  and the cardinality of the residue field corresponding to  $v$ .

$v$	$t_v^2 - 4N_v^2 \pmod{31}$	$u = t_v^2/N_v \pmod{31}$	$u^2 - 3u + 1 \pmod{31}$
$\mathfrak{p}_{11} = (\alpha - 2)$	3	24	9
$\mathfrak{q}_{11} = (-5\alpha^2 + \alpha - 3)$	17	19	26
$\mathfrak{q}_{13} = (-2\alpha + 1)$	14	17	22

Let  $s_1 := \rho_{E,31}(\mathrm{Frob}_{w_1})$  for any fixed  $w_1 \mid \mathfrak{p}_{11}$ ,  $s_2 := \rho_{E,31}(\mathrm{Frob}_{w_2})$  for any fixed  $w_2 \mid \mathfrak{q}_{13}$ , and  $t := \rho_{E,31}(\mathrm{Frob}_{w_3})$  for any fixed  $w_3 \mid \mathfrak{q}_{11}$ . In Proposition 2.12, take  $K := H(31)$ . By the above table and Proposition 2.12,  $H(31)$  contains  $\mathrm{SL}_2(\mathbb{F}_{31})$ . Since  $\det : H(31) \rightarrow \mathbb{F}_{31}^*$  is surjective, we have  $H(31) = \mathrm{GL}_2(\mathbb{F}_{31})$ . Then by Proposition 2.11,  $H_{31} = \mathrm{GL}_2(\mathbb{Z}_{31})$ .

Now consider the  $\ell = 3$  case. Consider the prime ideal  $\mathfrak{q}_{29} := (3\alpha^2 + 2)$  which lies over 29 and let  $\pi \in H_3$  be  $\rho_{E,3}(\mathrm{Frob}_w)$  for any  $w \mid \mathfrak{q}_{29}$ . Then for  $v = \mathfrak{q}_{29}$ ,  $N_v = 29$  and  $t_v = 6$  and hence the characteristic polynomial of  $\pi$  is  $t^2 - 6t + 29 \equiv (t - 7)(t - 8) \pmod{9}$ . The rest of the computation



for this case remains exactly the same as the  $\ell = 3$  case considered by Greicius in [Gre10]. Therefore  $H_3 = \text{GL}_2(\mathbb{Z}_3)$ .

Finally we consider the  $\ell = 2$  case. Recall that since  $[K(E[4]) : K] = 16$ ,  $H(4)$ , the mod 4 image is maximal. We will now use Proposition 2.9. Letting  $\mathfrak{p} := (157)$  in the proposition gives that  $\#(\mathcal{O}_K/\mathfrak{p}) = 3869893 \equiv 5 \pmod{8}$ . Computation in SAGE shows that  $E$  has full four-torsion over  $\mathcal{O}_K/\mathfrak{p}$ . This verifies that  $H_2 = V_1(2)$ .

The three conditions of Theorem 1.1 are now verified as desired.

*Remark.* We have written code in SAGE that automates the checking we did above and gives the prime ideals that one needs to satisfying the given conditions (see `check_sage.sws` in [CFLTL]).

### 3. CONSTRUCTING AN INFINITE FAMILY

Fix  $K = \mathbb{Q}(\alpha)$  where  $\alpha$  is the real root of  $x^3 + x + 1$ . In this section, we apply our criteria to obtain an *infinite* family of elliptic curves with maximal adelic image given full two-torsion over  $K$ . To do so, we obtain families of curves satisfying each of the requisite conditions:

- (i) semistability,
- (ii)  $K(E[4]) \cap K^{\text{cyc}} = K(i)$ , and
- (iii) maximal  $\ell$ -adic image for each prime  $\ell$ .

We are able to find congruence conditions on the coefficients of our elliptic curves ensuring each of these conditions, which we may then piece together using the Chinese remainder theorem.

Throughout this section, with  $b, c \in \mathbb{Z}$ , let  $E_{b,c}$  be the elliptic curve defined by

$$E_{b,c}/K : y^2 = x(x - (\alpha^2 + b\alpha + c))(x - 16(\alpha^2 + \alpha + 1)).$$

**3.1. A family of semistable elliptic curves.** Since the criteria we use for verifying maximality apply only to semistable curves, we must first find infinite families of semistable elliptic curves of the desired form. Such a family is furnished by the following proposition.

**Proposition 3.1.** *Suppose that one of the following two conditions is satisfied:*

- (i)  $b \equiv 5 \pmod{12}$  and  $c \equiv 4$  or  $8 \pmod{12}$ .
- (ii)  $b \equiv 9 \pmod{12}$  and  $c \equiv 4 \pmod{12}$ .

*Then*

$$E/K : y^2 = x(x - (\alpha^2 + b\alpha + c))(x - 16(\alpha^2 + \alpha + 1))$$

*is semistable.*

*Proof.* Since  $\mathcal{O}_K$  is a unique factorization domain, we will speak freely of primes of  $K$  as numbers. We establish the result for case (i). The proof for case (ii) is identical.

Let  $A = \alpha^2 + b\alpha + c$ ,  $B = 16(1 + \alpha + \alpha^2)$ , and  $C = A - B$ . We first claim that  $A$  and  $B$  are coprime in  $K$ . Since  $\alpha^3 + \alpha + 1 = 0$ ,  $1 + \alpha + \alpha^2 = \alpha^2 - \alpha^3 = \alpha^2(1 - \alpha)$ . Moreover,  $\alpha$  is a unit. Furthermore,  $N_{K/\mathbb{Q}}(1 - \alpha) = f(1) = 3$ . So  $1 + \alpha + \alpha^2$  is a prime lying over 3.

We also easily check that 2 is inert in  $K$ . Hence it suffices to prove that  $A$  is coprime to 2 and  $1 - \alpha$ . The former is clear. For the latter, observe that

$$A = \alpha^2 + b\alpha + c \equiv 1 + b + c \pmod{1 - \alpha}.$$

But  $b \equiv 2 \pmod{3}$  and  $c \equiv 1$  or  $2 \pmod{3}$ , so  $1 + b + c \not\equiv 0 \pmod{3}$ .

So we see that  $A$  and  $B$  are coprime, hence  $\{A, B, C\}$  are pairwise coprime. Now we note that for this Weierstrass form,

$$\Delta = 16(ABC)^2 \quad \text{and} \quad c_4 = 16(A^2 - AB + B^2)$$

If  $\mathfrak{p} \neq (2)$  is a prime dividing  $\Delta$ , then it divides exactly one of  $A, B, C$ . Supposing that  $\mathfrak{p} \mid A$ , we see that  $c_4 \equiv 16B^2 \not\equiv 0 \pmod{\mathfrak{p}}$ , so  $E$  is not semistable at  $\mathfrak{p}$ . Similarly, if  $\mathfrak{p} \mid B$  the curve is semistable at  $\mathfrak{p}$ . Finally, if  $\mathfrak{p} \mid C = A - B$ , then

$$c_4 = 16(A^2 - AB + B^2) \equiv 16A^2 \not\equiv 0 \pmod{\mathfrak{p}}.$$

The only prime left to consider is  $\mathfrak{p} = (2)$ . Making the change of variables  $(x, y) \mapsto (4x, 8y + 4\alpha^2x)$ , and noting that  $\alpha^4 = -\alpha(\alpha + 1)$ , we obtain the Weierstrass equation

$$y^2 + \alpha^2xy = x^3 + \frac{-A - B + \alpha(\alpha + 1)}{4}x^2 - \frac{AB}{16}x.$$

Since  $A = \alpha^2 + b\alpha + c$ , we see that  $A - \alpha - \alpha^2$  is divisible by 4, and hence the coefficients are in  $\mathcal{O}_K$ . For this Weierstrass form,  $\Delta = (ABC)^2/16$  and  $c_4 = A^2 - AB + B^2$ . Since  $2 \mid B$  and  $2 \nmid A$ , we see that  $E$  is semistable at 2 as well.  $\square$

**3.2. A family with maximal mod 4 image.** In this section, fix an elliptic curve  $E_{b,c}$ . To verify maximal 2-adic image, we must first have maximal mod 4 image and then apply Proposition 2.9. That  $\rho_4(G_K)$  is maximal is equivalent to  $[K(E[4]) : K] = 16$ . We will describe a procedure that may be used to determine congruence conditions on  $b$  and  $c$  which ensure that  $E$  has maximal mod 4 image. As an example, we prove the following:

**Proposition 3.2.** *Let*

$$E/K : y^2 = x(x - (\alpha^2 + b\alpha + c))(x - 16(\alpha^2 + \alpha + 1)),$$

*where  $b \equiv 3699 \pmod{4991}$  and  $c \equiv 4183 \pmod{4991}$ . Then  $\rho_{E,4}(G_K)$  is maximal.*

We emphasize that the congruence condition given in the proposition is just one of many possibilities. We begin with a general discussion. Recall that

$$K(E[4]) = K(x_1, x_2, x_3, \sqrt[4]{\Delta})$$

where  $x_1, x_2, x_3$  are the  $x$ -coordinates of 8-torsion point not differing by a 4-torsion point. We may take  $x_1, x_2, x_3$  to be the roots of the quadratics

$$\begin{aligned} x^2 - 16(b+c)\alpha^2 - 16(c-2)\alpha - 16(c-b-1) \\ x^2 - 32(\alpha^2 + \alpha + 1)x + 16((b+c)\alpha^2 + (c-2)\alpha + (c-b+1)) \\ x^2 + (-2\alpha^2 - 2b\alpha - 2c)x + 16(b+c)\alpha^2 + 16(c-2)\alpha + 16(c-b-1) \end{aligned}$$

which we obtained by factoring the 4-division polynomial for  $E$ , whose discriminants are, respectively,

$$\begin{aligned} d_1 &= 2^6((b+c)\alpha^2 + (c-2)\alpha + (c-b-1)) \\ d_2 &= 2^6(16(1+\alpha+\alpha^2)^2 - ((b+c)\alpha^2 + (c-2)\alpha + (c-b-1))) \\ d_3 &= 4(\alpha^2 + b\alpha + c)^2 - 64((b+c)\alpha^2 + (c-2)\alpha + (c-b-1)). \end{aligned}$$

In addition,

$$d_4 := \sqrt{\Delta} = 64(\alpha^2 + b\alpha + c)(\alpha^2 + \alpha + 1)(15\alpha^2 + (16-b)\alpha + (16-c)).$$

So

$$K(E[4]) = K(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3}, \sqrt{d_4}).$$

This is a degree 16 extension of  $K$  if and only if all 15 of the extensions  $K(\sqrt{N})$ , where  $N$  is the product of some non-empty subset of  $\{d_1, d_2, d_3, d_4\}$ , are nontrivial, or equivalently, if and only if all such  $N$  are not squares in  $\mathcal{O}_K$ .

So to ensure this, it suffices to find prime ideals  $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_4$  such that for each  $i = 1, 2, 3, 4$ , we have that  $d_i$  is a non-square in  $(\mathcal{O}_K/\mathfrak{p}_i)^\times$  and  $d_j$  is a square for  $j \neq i$ . If this is the case, then the product of any non-empty subset of  $d_1, d_2, d_3, d_4$  will fail to be a square in

$$(\mathcal{O}_K/\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4)^\times \simeq (\mathcal{O}_K/\mathfrak{p}_1)^\times \times (\mathcal{O}_K/\mathfrak{p}_2)^\times \times (\mathcal{O}_K/\mathfrak{p}_3)^\times \times (\mathcal{O}_K/\mathfrak{p}_4)^\times,$$

hence is obviously not a square in  $\mathcal{O}_K$ . Once ideals satisfying these conditions are found for a particular curve

$$E : y^2 = x(x - (\alpha^2 + b\alpha + c))(x - 16(\alpha^2 + \alpha + 1)),$$

where  $b, c \in \mathcal{O}_K$ , then they will work for any curve

$$E' : y^2 = x(x - (\alpha^2 + b'\alpha + c'))(x - 16(\alpha^2 + \alpha + 1)).$$

with  $b \equiv b' \pmod{\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4}$  and  $c \equiv c' \pmod{\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4}$ .

We carried out this program by computer search (see `test_primes.sws` in [CFLTL]). Many examples were found, but for brevity we simply list one.

*Proof of Proposition 3.2.* With  $b = 33645$  and  $c = 19156$ , the prime ideals

$$\mathfrak{p}_1 = (\alpha - 3), \quad \mathfrak{p}_2 = (7), \quad \mathfrak{p}_3 = (-\alpha^2 + 3\alpha - 1), \quad \mathfrak{p}_4 = (\alpha^2 + 4\alpha - 3)$$

satisfy the desired conditions. These lie over 31, 7, 31, and 23 respectively, so the congruence condition is over  $7 \times 23 \times 31 = 4991$ .  $\square$

**3.3. A family with  $K(E[4]) \cap K^{\text{cyc}} = K(i)$ .** In this section, we describe congruence conditions on  $b, c$  which ensure that  $E_{b,c}$  satisfies the field intersection condition

$$K(E[4]) \cap K^{\text{cyc}} = K(i).$$

Let  $d_1, d_2, d_3$ , and  $d_4$  be as Section 3.2. Collecting terms together, we find the following expressions.

(2)

$$d_3 = (16 + 14b - 16c + c^2) + (31 - 16c + 2bc - 2b)\alpha + (b^2 - 16b - 14c - 1)\alpha^2 := x + y\alpha + z\alpha^2$$

and

(3)

$$d_4 = -64(\alpha^2 + \alpha + 1)d_3.$$

Our key observation is that  $d_4$  can be divisible by only a few rational primes, which limits the possible intersection by Lemma 2.8. This is made precise in the proof of the proposition below.

**Proposition 3.3.** *Assume that*

$$(b, c) \not\equiv \begin{cases} (1, 1) & \text{or } (1, 2) & \pmod{3} \\ (1, 1) & \pmod{5} \\ (2, 5) & \pmod{11} \\ (4, 5) & \pmod{17} \\ (14, 11) & \text{or } (23, 6) & \text{or } (25, 9) & \pmod{31} \\ (467, 91) & \pmod{787} \\ (626, 280) & \pmod{827} \end{cases}$$

*Then  $E_{b,c}$  satisfies  $K(E_{b,c}[4]) \cap K^{\text{cyc}} = K(i)$ .*

*Proof.* Let  $\Delta_{b,c}$  denote the discriminant of  $E_{b,c}$ . Assume that  $b, c$  are such that  $K(E_{b,c}[4]) \cap K^{\text{cyc}} \neq K(i)$ . Then by Lemma 2.8, we have that  $K(\sqrt{n}) = K(\sqrt{m})$ , where  $n$  is an integer and  $m$  is a product of some subset of  $d_1, d_2, d_3, d_4$ . As  $n$  and  $m$  can only differ by a square of  $K$ , we have that some prime of  $\mathbb{Q}$  divides  $m$ , hence some prime  $p$  of  $\mathbb{Q}$  must divide  $d_1d_2d_3d_4$ .

Note that any prime of  $K$  dividing  $d_1, d_2, d_3$  must ramify in  $K(\sqrt{d_i})/K$ , and hence must divide  $\Delta_{b,c}$  (as we already have that  $2 \mid \Delta_{b,c}$ ). For primes of  $K$  not lying above 31, dividing  $\Delta_{b,c}$  is equivalent to dividing  $d_4$ . So  $p \mid d_1 d_2 d_3 d_4$  implies that either  $p \mid d_4$  or  $p = 31$  and  $p \mid \Delta_{b,c}$ .

Assume that  $p \mid d_4$ . Then, using (3), as  $\alpha^2 + \alpha + 1$  is a prime above 3, either  $p = 2, 3$ , or  $p \mid d_3$ . If  $p \mid d_3$ , then we must have that  $p \mid x, y, z$  (as defined in (2)), so  $p \mid c_x x + c_y y + c_z z$  for any  $c_x, c_y, c_z \in \mathcal{O}_K$ . We use  $c_x = 28, c_y = 8 - b, c_z = -2 + 2c$  to get that  $p \mid 698 + 377b - 550c$ . We use  $c_x = -4z - 56c - 260, c_y = y - 28b + 586, c_z = 56b + 4$  to get that  $p \mid 15027 - 4844b - 6328c$ . Putting these three conditions together, we get that  $p \mid 618889059855$ , and then factoring yields that  $p = 3, 5, 11, 17, 113, 787$ , or  $827$ .

Using the condition  $b \equiv 1 \pmod{4}, c \equiv 0 \pmod{4}$ , we get that  $2^6 \parallel d_1, 2^6 \parallel d_2, 2^2 \parallel d_3, 2^8 \parallel \Delta_{b,c}$ , so we can ignore powers of two when taking the square root.

Note that if for some choice of  $b, c$ ,  $p \nmid \Delta_{b,c}$ , then  $p \nmid \Delta_{b',c'}$  for any  $b', c' \equiv b, c \pmod{p}$ . Therefore, we can know which pairs  $(b, c)$  have no rational primes dividing  $(\Delta_{b,c})$  by simply checking if  $p \mid (\Delta_{b,c})$  for  $0 < b, c \leq p$  with  $p = 3, 5, 11, 17, 31, 113, 787, 827$  (see `bc_search.txt` in [CFLTL]).  $\square$

Therefore, by avoiding the above values, we can easily chose congruence conditions on  $b, c$  which will guarantee that no rational prime divides  $d_1 d_2 d_3 d_4$ , and hence  $K(E[4]) \cap K^{\text{cyc}} = K(i)$ . We choose  $(b, c)$  to be congruent to  $(2, 1) \pmod{3}, (2, 4) \pmod{5}, (6, 4) \pmod{11}, (0, 0) \pmod{17}$ , and  $(10, 29) \pmod{31}$ .

**3.4. A family with maximal  $\ell$ -adic image.** The tests for the remaining conditions can be easily modified into congruence conditions, as they all involve finding primes  $\mathfrak{p}$  of  $K$  such that  $\mathcal{O}_K/\mathfrak{p}$  and  $E \pmod{\mathfrak{p}}$  satisfy certain properties, all of which do not change if we fix the values of  $b, c \pmod{\mathfrak{p} \cap \mathbb{Z}}$ . We will simply state the primes used, as the calculations are analogous to those in Section 1.2.

**Proposition 3.4.** *Let  $b_0 = 17, c_0 = 4$ . If  $b, c \equiv b_0, c_0 \pmod{3 \cdot 5 \cdot 11 \cdot 29 \cdot 47}$ ,  $E_{b,c}$  has maximal mod 4 image, and  $E_{b,c}$  is semi-stable, then  $E_{b,c}$  has maximal  $\ell$ -adic image for all  $\ell$ .*

*Proof.* For a prime  $\mathfrak{p}$ , let  $E_{\mathfrak{p}}$  denote  $E_{b_0, c_0} \pmod{\mathfrak{p}}$ . First, we use the prime  $\mathfrak{p} = (\alpha^2 + \alpha + 2)$  and compute that  $\#E_{\mathfrak{p}}(K/\mathfrak{p}) = 2^3$ . Therefore  $E_{b_0, c_0}$ , the mod  $\ell$  representation is surjective for  $\ell \neq 2, 31$ . Since  $\mathfrak{p} \cap \mathbb{Z} = (3)$ , this shows that if  $b, c \equiv b_0, c_0 \pmod{3}$ , then the same holds for  $E_{b,c}$ .

To show that the mod 8 representation is maximal for  $E_{b_0, c_0}$ , we consider the prime  $\mathfrak{p} = (3\alpha^2 + 2)$ . As  $\mathfrak{p} \cap \mathbb{Z} = 29$ , the same is true for any curve with  $b, c \equiv b_0, c_0 \pmod{29}$ .

To show that the mod 9 representation is surjective for  $E_{b_0, c_0}$ , we use the prime  $\mathfrak{p} = (2\alpha^2 + \alpha + 4)$ , which lies above 47. If  $b, c \equiv b_0, c_0 \pmod{47}$ , the mod 9 representation is surjective for  $E_{b,c}$ .

Lastly, we must show that the mod 31 representation is surjective for  $E_{b_0, c_0}$ . We let  $w_1, w_2, w_3$  be primes such that  $w_1 \mid (-5\alpha^2 + \alpha - 3)$ ,  $w_2 \mid (5)$ , and  $w_3 \mid (\alpha^2 + \alpha + 2)$ . Since  $w_1 \cap \mathbb{Z} = 11, w_2 \cap \mathbb{Z} = 5, w_3 \cap \mathbb{Z} = 3$ , we have that if  $b, c \equiv b_0, c_0 \pmod{3 \cdot 5 \cdot 11}$ , the mod 31 representation is surjective.

Putting this together, we get, just as in the previous section, that the image of the mod  $\ell$  representation is maximal for all  $\ell$ .  $\square$

**3.5. Proof of Theorem 3.** We have already developed congruence conditions for each condition. We gather them together here. For convenience, we use the notation  $\cap, p$  to refer to the mod  $p$

congruence condition in Proposition 3.3.

Condition	$b$	$c$
semistable	5 (mod 12)	4 (mod 12)
mod 9	17 (mod 47)	4 (mod 47)
mod 4	3699 (mod $7 \cdot 13 \cdot 31$ )	4183 (mod $7 \cdot 13 \cdot 31$ )
mod 31	17 (mod $3 \cdot 5 \cdot 11$ )	4 (mod $3 \cdot 5 \cdot 11$ )
mod 8	17 (mod 29)	4 (mod 29)
$\ell$ -adic	2 (mod 3)	1 (mod 3)
$\cap, 3$	2 (mod 3)	1 (mod 3)
$\cap, 5$	2 (mod 5)	4 (mod 5)
$\cap, 11$	6 (mod 11)	4 (mod 11)
$\cap, 17$	0 (mod 17)	0 (mod 17)
$\cap, 31$	10 (mod 31)	29 (mod 31)
$\cap, 787$	0 (mod 787)	0 (mod 787)
$\cap, 827$	0 (mod 827)	0 (mod 827)

Using the Chinese remainder theorem, we put these together to get the congruence condition from the statement of the theorem. This completes the proof of Theorem 3.

#### 4. NON-SEMISTABLE ELLIPTIC CURVES AND NONTRIVIAL NARROW CLASS GROUP

Here we show how to extend Greicius's test for the surjectivity of the mod  $\ell$  representation to arbitrary elliptic curves  $E$  with non-integral  $j_E$ -invariant over arbitrary cubic number fields  $K$ . In particular, we do not need to suppose that the elliptic curve  $E$  is semistable over  $K$ .

To fix notation, we let  $\Sigma_K$  denote the set of primes of  $K$  for a number field  $K$ . We let  $S_E \subseteq \Sigma_K$  be the set of primes of bad reduction of the elliptic curve  $E/K$ , and we let  $S_\ell$  be the set of primes above the rational prime  $\ell$ . For a prime  $v \in \Sigma_K$ , we let  $I_v \subseteq G_K$  denote the inertia subgroup at  $v$ . If  $w$  is a prime lying over  $v$ , we denote by  $f(w/v), e(w/v)$  the residue degree and ramification index of  $w$  over  $v$ , respectively. If a Galois extension is unramified at  $v$ , we denote by  $\text{Frob}_v$  the Frobenius element of  $v$  in the Galois group of that extension. We let  $U_v$  denote the  $v$ -adic units,  $\mathcal{O}_v$  the completion of  $\mathcal{O}_K$  at  $v$ , and  $\mathfrak{m}_v$  the maximal ideal of  $\mathcal{O}_v$ . We let  $U_K$  denote the group of units of  $\mathcal{O}_K$ , and we let  $U_K^+$  denote the subgroup of totally positive units. For a modulus  $\mathfrak{m}$ , in the sense of class field theory, we let  $U_{\mathfrak{m},1} = U_K \cap K_{\mathfrak{m},1}$ . All of this notation is identical to that of [Gre10] where applicable.

By a *half-Borel* subgroup of  $\text{GL}_2(\mathbb{F}_\ell)$  we mean a subgroup stabilizing a subspace of  $\mathbb{F}_\ell^2$  and acting trivially on either the subspace or the quotient by it. In other words, some conjugate of the subgroup lies in the set of matrices of the form

$$\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}.$$

*Remark.* Throughout this section, words such as “larger,” “smaller,” and “bounded” are used in the sense of divisibility rather than absolute value.

To begin, we recall some useful results from [Gre10]. In [Gre10, Lemma 3.4], Greicius summarizes some results from [Ser72] on the inertia representation for the case of semistable elliptic curves. We restate these results, but note that most of the results only depend on the curve being semistable at a particular prime.

**Lemma 4.1** ([Ser72]). *Let  $K$  be a number field,  $\ell$  a rational prime, and  $E/K$  an elliptic curve with  $j$ -invariant  $j_E$ . Fix  $v \in \Sigma_K$  and  $w \in \Sigma_{\overline{K}}$  with  $w \mid v$ .*

*First, suppose  $v \notin S_E$ .*

(i) *If  $v \notin S_\ell$ , then  $\rho_{E,\ell}(I_w)$  is trivial.*

Suppose for the next two that  $\ell$  is unramified in  $K$ .

- (ii) If  $v \in S_\ell$ , and  $E$  has ordinary reduction at  $v$ , then the image of  $D_w$  is contained in a Borel subgroup, and  $I_w$  acts via the trivial character and via a character of order  $p - 1$ .
- (iii) If  $v \in S_\ell$ , and  $E$  has supersingular reduction at  $v$ , then the image of  $I_w$  is a non-split Cartan subgroup.

Suppose, furthermore, that  $E$  is semistable at  $v$ .

- (iv) If  $v \in S_E \setminus S_\ell$ , then  $\rho_{E,\ell}(I_w)$  is trivial or cyclic of order  $\ell$ .
- (v) If  $v \in S_E$ ,  $\ell \nmid v(j_E)$ , then  $\rho_{E,\ell}(I_w)$  contains an element of order  $\ell$ .
- (vi) If  $v \in S_\ell$  and  $\ell$  is unramified in  $K$ , then  $\rho_{E,\ell}(I_w)$  is a half Borel subgroup.

*Proof.* Assume first that  $\ell$  is not ramified in  $K$ . Everything except (ii) and (iii) are stated in [Gre10, Lemma 3.4]. The remaining two follow from the content of [Ser72, Section 1.11].

If  $\ell$  is ramified in  $K$ , (i) follows from the Criterion of Néron-Ogg-Shafarevich, and (iv) follows by examining the Tate curve as in [Ser98, IV.A.1.5].  $\square$

As in [Gre10], we have the following:

**Proposition 4.2.** *Suppose  $E/K$  is an elliptic curve with  $j$ -invariant  $j_E$ , and suppose  $\ell$  is a prime that does not ramify in  $K$  such that  $\ell \nmid v(j_E)$  for some place  $v$  of multiplicative reduction. If  $\rho_{E,\ell}(G_K) \neq \mathrm{GL}_2(\mathbb{F}_\ell)$ , then  $\rho_{E,\ell}(G_K)$  is contained in a Borel subgroup of  $\mathrm{GL}_2(\mathbb{F}_\ell)$ .*

*Proof.* By Lemma 4.1(v), we know that the mod  $\ell$  image contains an element of order  $\ell$ . It thus must either contain  $\mathrm{SL}_2(\mathbb{F}_\ell)$  or be contained in a Borel subgroup (see [Ser98, IV.3.2, Lemma 2]). As  $\ell$  does not ramify in  $K$ , the intersection of  $K$  with  $\mathbb{Q}(\mu_{\ell^\infty})$  is  $\mathbb{Q}$  as  $\ell$  does not ramify in  $K$ , so the determinant modulo  $\ell$  is surjective. Therefore, in the former case, the image is  $\mathrm{GL}_2(\mathbb{F}_\ell)$ .  $\square$

*Remark.* In practice, we find elliptic curves with one  $v$  such that  $v(j_E) = -1$ , so that  $v$  works for all  $\ell$ . However, one can extend the result to other elliptic curves, if necessary by checking explicitly other  $\ell$  using Proposition 2.12. Also note that if  $\ell \neq 2, 3$  (or just  $\ell \neq 2$  if  $E$  has full 2-torsion over  $K$ ), we only need  $v$  to be potentially multiplicative, since, as we will see below,  $E$  becomes semistable over an extension of degree divisible only by the primes 2 and 3.

Assuming  $\ell \nmid v(j_E)$  for  $v$  multiplicative, let us suppose that the mod  $\ell$  representation is not surjective. It follows that the representation  $\rho_{E,\ell}$  takes the form

$$\begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$$

in some basis of  $E[\ell]$ , where  $\chi_1, \chi_2$  are characters from  $G_K$  into  $\mathbb{F}_\ell^\times$ . Note that the Borel subgroup and hence the characters depend purely on the 1-dimensional vector subspace of  $E[\ell]$  left invariant by that subgroup. We call these the *isogeny characters relative to that subspace*.

In fact, the pair of isogeny characters is independent of which subspace we choose. Although we will not truly need this fact until Lemma 4.10, we prove it now.

**Lemma 4.3.** *The set of isogeny characters  $\{\chi_1, \chi_2\}$  is independent of the basis for our Borel subgroup.*

*Proof.* We can view  $E[\ell]$  as a module over the ring  $R := \mathbb{F}_\ell[G_K]$  via the representation. If the image is contained in a Borel subgroup, then it is reducible, i.e. there is some subspace  $W \subseteq E[\ell]$  which is an  $R$ -submodule of  $E[\ell]$ . The  $R$ -modules  $W$  and  $E[\ell]/W$  correspond to the characters  $\chi_i$ . But if  $W'$  is a different submodule, then the set of  $R$ -modules  $\{W, E[\ell]/W\}$  equals the set  $\{W', E[\ell]/W'\}$  by the Jordan-Hölder theorem. It follows that the characters, and in particular, whether they ramify at a given prime of  $K$ , are independent of  $W$ .  $\square$

In [Gre10], Greicius shows that in the situation above, if  $E$  is semistable, and  $K$  satisfies certain technical properties, then one of these isogeny characters is unramified. In that case, because the narrow class group of  $K$  is trivial, that character is trivial. Greicius uses this to show that  $\ell$  divides the number of points modulo any prime of good reduction.

As stated earlier, we would like to extend his results ruling out all but finitely many  $\ell$  to non-semistable curves and more general  $K$ . In order to do this, we would like to analyze how much the two characters  $\chi_1, \chi_2$  can ramify.

First, we briefly note what happens at semistable primes not dividing  $\ell$ .

**Lemma 4.4.** *Suppose that  $\rho_\ell: G_K \rightarrow \mathrm{GL}(E[\ell])$  is contained in a Borel subgroup. Then the isogeny characters are unramified at any  $v \notin S_\ell$  at which  $E$  has semistable reduction.*

*Proof.* If  $E$  has good reduction at  $v$ , then  $\rho_\ell$  itself is unramified. If  $E$  has multiplicative reduction at  $v$ , we know by Lemma 4.1 that the image of  $I_v$  has order dividing  $\ell$ . As the characters have codomain  $F_\ell^\times$ , which has order  $\ell - 1$ , the characters are trivial on  $I_v$ .  $\square$

**4.1. Non-semistability.** Next, we would like to tackle the primes at which  $E$  is not semistable. We will only cover those primes not dividing  $\ell$ , then assume at the end that  $\ell$  is a rational prime not lying under any prime of additive reduction.

We say that an elliptic curve  $E/K$  is *Legendre* over  $K$  if  $E$  is isomorphic over  $K$  to a curve in Legendre form  $y^2 = x(x-1)(x-\lambda)$ . If the elliptic curve  $y^2 = f(x)$ , where  $f$  is a cubic polynomial over  $K$ , has full 2-torsion over  $K$ , then we can write the equation in the form

$$y^2 = (x-a)(x-b)(x-c)$$

with  $a, b, c \in K$ . Over  $\overline{K}$ , the curve can be written in Legendre form, but that does not mean that the curve is Legendre over  $K$ . More precisely, we have the following well known fact (see Proposition III.1.7 in [Sil09]).

**Lemma 4.5.** *If  $E/K$  is an elliptic curve defined by equation  $y^2 = (x-e_1)(x-e_2)(x-e_3)$  over  $K$  (which happens if  $E$  has full 2-torsion over  $K$ ), then  $E$  is Legendre over  $L = K(\sqrt{e_1-e_2})$ . (By symmetry, this means we can take  $L = K(\sqrt{e_i-e_j})$  for some  $i \neq j$ .)*

In order to deal with non-semistability, we would like to know over what field the curve becomes semistable. A general result says that this is true for an abelian variety if we adjoin the 12-torsion. However, in the case of elliptic curves, we have the following lemma

**Lemma 4.6.** *Suppose  $E/K$  is an elliptic curve with full 2-torsion over  $K$  and additive reduction at  $v \in \Sigma_K$ . Then:*

- *If  $E$  has potentially good reduction at  $v$ , then there is an extension  $L/K$  of ramification index at most 2 over which  $E$  has good reduction.*
- *If  $E$  has potentially multiplicative reduction at  $v$ , then there is an extension  $L/K$  of ramification index at most 4 over which  $E$  has multiplicative reduction.*

*Furthermore, suppose  $E$  is Legendre over  $L/K$ . If  $v$  does not ramify in  $L$ , then the above indices are 1 and 2, respectively.*

*Proof.* By the proof of Proposition 5.4 in [Sil09, Chapter VII], a Legendre curve has good reduction at all primes of potentially good reduction, and otherwise has multiplicative reduction at  $v$  after adjoining the square root of a uniformizer at  $v$ . Finally, a curve with full 2-torsion becomes Legendre over an at most quadratic extension of  $K$ .  $\square$

We know that over some extension  $L/K$ , one of the characters is trivial. Therefore, we could count the points over the residue fields of  $L$  and take the greatest common divisor of these values. We should note first that computing in number fields is ineffective and impractical. Therefore, it

makes more sense to compute  $[L : K]$  and then take the unique finite field of that degree (over the residue field of  $K$ ), then compute the number of points of our elliptic curve over that finite field.

In order to trivialize one of the characters, one could take a field over which  $E$  is semistable. Over this extension and under the conditions above, one of our characters would be unramified at every finite prime not dividing  $\ell$ . It would follow that that character becomes trivial over the narrow Hilbert class field of this extension. However, the analysis of primes dividing  $\ell$  does not work over this field, which means that we must find a different method.

We put bounds on the ramification of non-semistable primes at each of these characters. Then, since the extensions defined by the characters are abelian, they have conductors by class field theory, and we can use these bounds on the ramification indices to control the conductor of this extension. Therefore, assuming one of the characters is unramified at all primes of semistable reduction, the character is trivialized over the ray class field associated to this conductor.

One advantage is that the splitting of primes in the ray class field is described explicitly by the Artin reciprocity law, so we can actually bound the order of the image of the Frobenius element under the character. Note that MAGMA can compute the order of a given ideal in the ray class group, so this method can be easily implemented. Finally, note that once we fix the field  $K$ , the computation of the ray class group for different moduli  $\mathfrak{m}$  is very easy by the exact sequence

$$1 \rightarrow U_K^+ / U_{\mathfrak{m},1} \rightarrow (\mathcal{O}_K / \mathfrak{m})^\times \rightarrow \mathcal{C}_K^{\mathfrak{m}} \rightarrow \mathcal{C}_K^\infty \rightarrow 1,$$

the only difficult part being computing the narrow class group. Conversely, the method outlined above involves computing an ideal class group that depends on the modulus and hence on the elliptic curve. Therefore, if one is working with many elliptic curves over the same field, our method works much better.

We suppose for simplicity from now on that 2 does not ramify in  $K$ . We also suppose for the next two sections that the mod  $\ell$  representation is contained in some (fixed) Borel subgroup, hence has isogeny characters  $\chi_i$  for  $i = 1, 2$ .

#### 4.2. Curves with full 2-torsion.

**Lemma 4.7.** *Let  $E/K$  have full 2-torsion over  $K$ . Suppose  $v \notin S_\ell$ . Then the following are true*

- (1) *If  $v \notin S_2$ , each character  $\chi_i$  is not wildly ramified at  $v$ , and if  $v \in S_2$ , each character is ramified of index dividing 4.*
- (2) *If  $v \in S_2$  does not ramify in an extension over which  $E$  is Legendre, or is of potentially good reduction, the index is 2 (or 1 if both happen).*

*Proof.* By Lemma 4.4, we know that if  $E$  has semistable reduction at  $v$ , then both characters are unramified at  $v$ .

By Lemma 4.6, the curve becomes semistable at  $v$  over an extension of degree 4 obtained by first putting the curve in Legendre form (which happens over some quadratic extension) and then adjoining the square root of a uniformizer at  $v$ . If it is potentially good at  $v$ , this happens after obtaining Legendre form. Over this extension,  $E$  is semistable at  $v$ , so both of the isogeny characters are unramified at  $v$  by Lemma 4.4. If  $v \nmid 2$ , this means that the extension is not wildly ramified at  $v$ . If  $v \mid 2$ , the above follows immediately from the description of the field over which  $E$  becomes semistable at  $v$  in Lemma 4.6.  $\square$

We recall that for a place  $v$  and an abelian extension  $L/K$ , there is a “conductor” of the extension at  $v$ , which is the smallest power  $\mathfrak{m}_v^k$  of  $\mathfrak{m}_v$ , the maximal ideal at  $v$ , such that  $1 + \mathfrak{m}_v^k$  is in the kernel of the local Artin map. The conductor of a character  $\chi_i$  is the conductor of the extension defined by  $\chi_i$ . The *global conductor* is the product of the local conductors. An abelian extension of given global conductor is contained in the ray class field associated to that conductor, and a character with that global conductor is trivial over that ray class field. We say that the conductor of  $L/K$  outside a set  $S \subseteq \Sigma_K$  is the product of the local conductors at all  $v \notin S$ .



**Proposition 4.8.** *Suppose  $E$  is Legendre over  $L/K$ . For  $v \in S_2$ , let  $r(v) = 3$  if  $v$  ramifies in  $L$  or  $E$  has potentially multiplicative reduction at  $v$ , 0 otherwise. Let  $s(v) = 1$  if  $f(v/2) = 1$ ,  $v$  ramifies in  $L$ , and  $E$  has potentially multiplicative reduction at  $v$ , and 0 otherwise. Then let*

$$i(v) := \begin{cases} 0 & \text{if } E \text{ is semistable at } v, \\ 0 & \text{if } E \text{ has additive potentially good reduction at } v, \\ & v \text{ does not ramify in } L, \text{ and } v \nmid 2, \\ 1 & \text{if } E \text{ has additive reduction at } v \text{ and } v \nmid 2 \text{ otherwise.} \\ r(v) + s(v) & \text{otherwise.} \end{cases}$$

Then if we let  $\mathfrak{m}_f = \prod_{v \in \Sigma_K} v^{i(v)}$  and  $\mathfrak{m}$  the product of  $\mathfrak{m}_f$  with all real places, the conductor of the extension defined by  $\chi_i$  is at most  $\mathfrak{m}$  outside  $S_\ell$ .

*Proof.* Lemma 4.7 gives us bounds on the ramification of the extension defined by the characters. We need only translate these into bounds on the conductor of the extension.

As mentioned, the extension is unramified at any primes of semistable reduction. We also know the extension is unramified at  $v$  if  $v$  does not ramify in  $L$  and is potentially good. Furthermore, as the index is a power of 2, it is tamely ramified at all primes other than 2. This means that the conductor has exponent at most 1 at that prime.

In the case of  $v \mid 2$ , we use the description of the local Artin map to compute the conductor. The image of  $U_v$  under the local Artin map is the inertia group at  $v$  in the extension, and we know that this image is of order bounded by 4 (respectively, 2), so its kernel has index at most 4 (respectively, 2). We thus wish to classify subgroups of  $U_v$  of index at most 4 or 2. Since 2 is not ramified in  $K$ , the  $v$ -adic exponential converges for  $|x|_v < 1/2$ , meaning that  $1 + \mathfrak{m}_v^2 \mathcal{O}_v$  is isomorphic to  $\mathcal{O}_v$  as a topological group. This latter is pro-cyclic, hence has a unique open subgroup of given index. If the index is at most 4, and  $f(v/2) > 1$ , then  $(1 + \mathfrak{m}_v^2 \mathcal{O}_v)/(1 + \mathfrak{m}_v^3 \mathcal{O}_v)$  has order at least 4, so this kernel contains  $1 + \mathfrak{m}_v^3 \mathcal{O}_v$ , and the conductor is at most  $\mathfrak{m}_v^3$  at  $v$ .

In the case that the index is only bounded by 4 (by the previous proposition), and  $f(v/2) = 1$ , then  $(1 + \mathfrak{m}_v^2 \mathcal{O}_v)/(1 + \mathfrak{m}_v^4 \mathcal{O}_v)$  has order 4, so the conductor is bounded by  $\mathfrak{m}_v^4$  at  $v$ .  $\square$

*Remark.* If one does not wish to compute  $L$  above, one can always suppose that  $v$  ramifies in  $L$ . Then  $r(v)$  is always 3, and  $s(v) = 1$  if  $v(j) < 0$  and  $f(v/2) = 1$ , and  $s(v) = 0$  otherwise. This is what we did in our calculations. However, we included the most general result for completeness, and because it may reduce the computation time for much larger fields.

**4.3. General curves.** We now do not assume the curve has full 2-torsion in order to apply our results to the search for curves whose adelic representation is surjective. Once again, we suppose from now on for simplicity that 3 does not ramify in  $K$ .

We know that after passing to a degree 6 extension, the curve has full 2-torsion. It follows that, after passing to an extension of degree at most 24, our curve becomes semistable. We therefore get the same bounds for ramification indices as in Lemma 4.7, but we must multiply each of them by 6. We translate these into bounds on the conductor of the character:

**Proposition 4.9.** *For  $v \in S_2$ , let  $r(v) = 2$  if  $E$  has potentially good reduction at  $v$  and  $r(v) = 3$  if  $E$  has potentially multiplicative reduction at  $v$ .*

$$i(v) := \begin{cases} 0 & \text{if } E \text{ is semistable at } v, \\ 1 & \text{if } E \text{ has additive reduction at } v \text{ and } v \nmid 6, \\ 2 & \text{if } E \text{ has additive reduction at } v \text{ and } v \in S_3, \\ 2 + \left\lceil \frac{r(v)}{f(v/2)} \right\rceil & \text{if } E \text{ has additive reduction at } v \text{ and } v \in S_2. \end{cases}$$

Then if we let  $\mathfrak{m}_f = \prod_{v \in \Sigma_K} v^{i(v)}$  and  $\mathfrak{m}$  the product of  $\mathfrak{m}_f$  with all real primes, then the conductor of the extension defined by  $\chi_i$  is at most  $\mathfrak{m}$  outside  $S_\ell$ .

*Proof.* Once again, if  $E$  is semistable at  $v$ , there is no ramification. If  $v \nmid 6$ , then the ramification is not wild at  $v$ , so the conductor has power at most 1 at  $v$ .

As for  $v \mid 3$ , the  $v$ -adic logarithm shows that  $1 + \mathfrak{m}_v \mathcal{O}_v \cong \mathcal{O}_v$  as topological groups (assuming that 3 does not ramify in  $K$ ), so the kernel of the character must contain  $1 + \mathfrak{m}_v \mathcal{O}_v$ .

Finally, if  $v \mid 2$ , then (assuming 2 does not ramify in  $K$ ), the group  $1 + \mathfrak{m}_v^2 \mathcal{O}_v$  is pro-cyclic, and  $(1 + \mathfrak{m}_v^k \mathcal{O}_v)/(1 + \mathfrak{m}_v^{k+1} \mathcal{O}_v)$  has order  $f(v/2)$ , so the exponent of the conductor is at most  $2 + \lceil r(v)/f(v/2) \rceil$  if the 2-part of the ramification index is at most  $2^{r(v)}$ . The values of  $r(v)$  follow from the values from the previous section, but with ramification indices multiplied by 6.  $\square$

**4.4. Cubic Fields.** Next, we deal with  $v \in S_\ell$ . In [Gre10], Greicius uses Corollary 3.6 to analyze this case. This relies on the fact that  $K = \mathbb{Q}(\alpha)$ ,  $\alpha^3 + \alpha + 1 = 0$ ,  $\alpha \in \mathbb{R}$  has trivial narrow class group and the fact that there exists a totally positive unit  $u$  of  $K$  such that  $u - 1$  is also a unit. To extend his result, we prove the following proposition for general cubic fields:

**Lemma 4.10.** *Let  $E/K$  be an elliptic curve over a cubic field  $K$ , and let  $\ell$  satisfy the conditions of Proposition 4.2 and not lie below any primes of additive reduction for  $E$ . Let  $u$  be a positive fundamental unit of  $K$ . Let  $k$  be the smallest positive power of  $u$  contained in  $U_{\mathfrak{m},1}$ . Let  $d := \#C_K^\infty$  denote the order of the narrow class group of  $K$ . Let  $r := \#(\mathcal{O}_K/\mathfrak{m}_f)^\times$ , where  $\mathfrak{m}$  is defined as above, depending on whether  $E$  has full 2-torsion over  $K$ . Suppose that*

$$\ell \nmid N_{K/\mathbb{Q}} \left( \prod_{i=1}^{dr/k} u^{ik} - 1 \right).$$

*Then one of the characters  $\chi_i$  is unramified at every semistable  $v \in S_\ell$ .*

*Proof.* We divide our argument into cases based on the splitting of  $\ell$  in  $K$ .

Case 1:  $\ell$  is inert. Then there is a unique place  $v$  of  $K$  above  $\ell$ . As the image of  $\rho_\ell$  contains an element of order  $\ell$ , the image cannot be contained in a non-split Cartan subgroup, so  $E$  has ordinary or bad reduction at  $v$  by Lemma 4.1(iii). In each case, Lemma 4.1 tells us that the image of inertia is a half-split Cartan subgroup or a half-Borel subgroup, implying that the character is unramified at  $v$ .

Case 2:  $\ell$  splits completely. Suppose  $(\ell) = \mathfrak{p}\mathfrak{q}\mathfrak{r}$ . By the previous case, we see that each prime above  $\ell$  is unramified at at least one of the characters. By the pigeonhole principle, one of the characters, say  $\chi_i$ , is unramified at at least two of the primes above  $\ell$ . Suppose without loss of generality that it is unramified at  $\mathfrak{q}$  and  $\mathfrak{r}$ , and suppose it is ramified at  $\mathfrak{p}$ .

As  $\#\mathbb{F}_\ell^\times = \ell - 1$ , which is prime to  $\mathfrak{p}$ , the character  $\chi_i$  is not wildly ramified at  $\mathfrak{p}$ . Its conductor is therefore at most  $\mathfrak{m}\mathfrak{p}$ , by either Proposition 4.8 or Proposition 4.9, respectively. It follows that  $\chi_i$  factors through the ray class field  $L_{\mathfrak{m}\mathfrak{p}}$ , i.e. it factors through  $\mathcal{C}_K^{\mathfrak{m}\mathfrak{p}}$  under the Artin map. Now, we have an exact sequence

$$1 \rightarrow U_K^+/U_{\mathfrak{m}\mathfrak{p},1} \rightarrow (\mathcal{O}_K/\mathfrak{m}_f\mathfrak{p})^\times \rightarrow \mathcal{C}_K^{\mathfrak{m}\mathfrak{p}} \rightarrow \mathcal{C}_K^\infty \rightarrow 1.$$

Suppose that  $\chi_i$  is ramified at  $\mathfrak{p}$ . By the hypothesis,  $u^{ik} - 1$  is prime to  $\ell$ , hence not divisible by  $\mathfrak{m}_f\mathfrak{p}$ , for all  $ik \leq dr$ . For  $i$  such that  $k \nmid i \leq dr$ , we know that  $u^i - 1$  is not divisible by  $\mathfrak{m}_f\mathfrak{p}$ . Therefore, we know that  $u$  has order greater than  $dr$  in  $U_K^+/U_{\mathfrak{m}\mathfrak{p},1}$ , and the same is true of its image in  $(\mathcal{O}_K/\mathfrak{m}\mathfrak{p})^\times$ . Now,  $(\mathcal{O}_K/\mathfrak{m}_f\mathfrak{p})^\times \cong (\mathcal{O}_K/\mathfrak{m}_f)^\times \times (\mathcal{O}_K/\mathfrak{p})^\times$  as  $\ell$  does not lie below any primes of additive reduction, hence any primes dividing  $\mathfrak{m}$ . This means that

$$\#(\mathcal{O}_K/\mathfrak{m}_f\mathfrak{p})^\times = \ell r.$$

As  $u$  has order greater than  $dr$ , the cokernel of

$$U_K^+/U_{\mathfrak{m}\mathfrak{p},1} \rightarrow (\mathcal{O}_K/\mathfrak{m}_f\mathfrak{p})^\times$$

has order less than  $\ell/d$ .

Let  $\mathcal{D}$  denote this cokernel. By our exact sequence above,  $\mathcal{D}$  is also equal to the kernel of the surjection  $\mathcal{C}_K^{\text{mp}} \rightarrow \mathcal{C}_K^\infty$ . Then  $\mathcal{D}$  has index  $d = \#\mathcal{C}_K^\infty$  in  $\mathcal{C}_K^{\text{mp}}$ . Since  $\chi_i: \mathcal{C}_K^{\text{mp}} \rightarrow \mathbb{F}_\ell^\times$  is surjective, the image of  $\mathcal{D}$  in  $\mathbb{F}_\ell^\times$  has index at most  $d$ , hence is of order at least  $\ell/d$ . But we have already shown that  $\mathcal{D}$  has order less than  $\ell/d$ , so it cannot surject onto a group of order at least  $\ell/d$ . This contradiction shows that  $\chi_i$  cannot be ramified at  $\mathfrak{p}$ .

Case 3:  $\ell$  splits as  $\mathfrak{p}\mathfrak{q}$  where  $f(\mathfrak{p}/\ell) = 1$ . Then one of the characters is unramified at  $\mathfrak{q}$ , so we apply the same argument with that character at  $\mathfrak{p}$  to show that it cannot be ramified at  $\mathfrak{p}$ .

This completes the proof.  $\square$

*Remark.* If  $K = \mathbb{Q}$ , the lemma is automatically true because only Case 1 can occur.

We now combine our results into the following.

**Theorem 4.11.** *Let  $E/K$  be an elliptic curve over a cubic field  $K$  not Galois over  $\mathbb{Q}$ . If  $E$  has full 2-torsion over  $K$ , let  $\mathfrak{m}$  be as in Proposition 4.8, and otherwise, let  $\mathfrak{m}$  be as in Proposition 4.9. Let  $\ell$  be a prime of  $\mathbb{Q}$  such that:*

- (1)  $\ell$  does not ramify in  $K$
- (2) There is a prime  $v$  at which  $E$  has semistable reduction and such that  $\ell \nmid v(j_E) < 0$
- (3)  $\ell$  does not lie below any primes of  $K$  at which  $E$  is not semistable
- (4) We have that

$$\ell \nmid N_{K/\mathbb{Q}} \left( \prod_{i=1}^{dr/k} u^i - 1 \right),$$

where  $d := \#\mathcal{C}_K^\infty$ ,  $r := \#(\mathcal{O}_K/\mathfrak{m}_f)^\times$ ,  $u$  is a positive fundamental unit of  $K$ , and  $k$  is the order of  $u$  in  $U_{K,1}^+/U_{\mathfrak{m},1}$

If  $\rho_\ell(G_K) \subsetneq \text{GL}_2(\mathbb{F}_\ell)$ , then one of the characters  $\chi_i$  is trivial over the ray class field  $L_{\mathfrak{m}}$  of  $K$  of conductor  $\mathfrak{m}$ .

*Proof.* By Proposition 4.2, the first two conditions on  $\ell$  imply that the characters exist. Proposition 4.8 or Proposition 4.9, respectively, shows that character has conductor  $\mathfrak{m}$  outside of  $S_\ell$ . The third condition means that  $E$  is semistable at all of  $S_\ell$ , so Lemma 4.10 implies that one of the characters  $\chi_i$  is unramified at all of  $S_\ell$ . As it is unramified at  $S_\ell$ , we know that  $\mathfrak{m}$  is its conductor, and thus it is trivial over  $L_{\mathfrak{m}}$ .  $\square$

**Corollary 4.12.** *Let  $\mathfrak{m}$ ,  $E/K$ , and  $\ell$  be as above, and let  $n$  be the order of  $v$  in  $\#\mathcal{C}_K^{\mathfrak{m}}$ , where  $v \nmid \mathfrak{m}$  is a prime of good reduction. Let  $l_v$  be the unique degree  $n$  extension of  $k_v$ . Then if  $\rho_{E,\ell}(G_K) \neq \text{GL}_2(\mathbb{F}_\ell)$ , we have  $\ell \mid \#\tilde{E}_v(l_v)$  (equivalently, the reduced curve has an  $\ell$ -torsion point).*

*Proof.* This argument follows [Gre10, Proposition 3.8] almost identically.  $\square$

*Remark.* Note that this is also true if we replace  $n$  by one of its multiples, since then we only get a larger  $l_v$ . In particular, if we do not wish to compute the order of  $v$  in the ray class group, we can just let  $n$  always equal  $\#\mathcal{C}_K^{\mathfrak{m}}$ .

This gives us an efficient way to test for surjective image. In searching for examples, we restricted our attention to those  $E$  with multiplicative reduction at a prime  $v$  such that  $v(j_E) = -1$ . For the other  $\ell$ , we use Proposition 2.12.

*Remark.* We can replace (2) in each criterion with  $v$  potentially multiplicative, as explained in Remark 4. Therefore, in most generality, our method extends to arbitrary elliptic curves with non-integral  $j$ -invariant over arbitrary cubic (and quadratic) fields  $K$ .

**4.5. Further examples.** In this section we briefly mention two examples that result from our theory developed above. These examples were found using Theorem 4.11 and Corollary 4.12 and methods similar to Section 3.4 of [Gre10] and Example 1.2. Due to the similarities, we content ourselves with just briefly mentioning the proof.

We first give an example of a non-Galois cubic field  $K$  and an elliptic curve  $E/K$  with full 2-torsion over  $K$  which has maximal adelic Galois image, but is not semistable.

**4.5.1. Proof of Example 1.4.** Let  $\beta$  be the unique real root of  $x^3 + 4x^2 + 7x - 4$  and  $K = \mathbb{Q}(\beta)$ . We want to show that the adelic representation  $\rho_E$  associated to the elliptic curve

$$E/K: y^2 = x(x + (10\beta^2 - 3))(x - (\beta + 4))$$

surjects onto  $V_1(2) \times \prod_{\ell > 2} \mathrm{GL}_2(\mathbb{Z}_\ell)$ .

Let  $H := \rho_E(G_K)$ . Note that the discriminant of  $K$  is  $-503$ ,  $5\beta^2 + 9\beta - 5$  is a totally positive unit of  $K$ , and  $\mathfrak{m}_f = ((3/2)\beta^2 + (13/2)\beta + 13)^3$ . In condition (4) of Theorem 4.11 we will be inefficient and take  $k = 1$ . Conditions (1), (3), and (4) of Theorem 4.11 imply that  $H(\ell) = \mathrm{GL}_2(\mathbb{F}_\ell)$  for  $\ell \neq 2, 5, 17, 41, 73, 211, 503, 2143, 2269, 3907, 5449, 31741, 40471, 493333, 938251, 1225603, 1315849, 37012153$ . To show that  $H(\ell) = \mathrm{GL}_2(\mathbb{F}_\ell)$  for these remaining  $\ell \neq 2$ , we use Proposition 2.12. Then proceeding as in Example 1.2 shows that  $\rho_E$  surjects onto  $V_1(2) \times \prod_{\ell > 2} \mathrm{GL}_2(\mathbb{Z}_\ell)$ . (See `nonsemi_magma.txt` and `nonsemi_sage.sws` in [CFLTL] for results of computations.)  $\square$

We end by noting that the methods we developed in Section 4 can also be used to consider the case of surjective  $\rho_E$  when the narrow class group is nontrivial. We offer the following example.

**4.5.2. Proof of Example 1.5.** Let  $\beta$  be the unique real root of  $x^3 + 8x^2 - 3x + 1$  and  $K = \mathbb{Q}(\beta)$ . We show that with

$$E/K: y^2 + xy + \beta y = x^3 - 8x^2 - 6x - 1$$

the corresponding  $\rho_E$  surjects onto  $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ .

Again as above, let  $H := \rho_E(G_K)$ . We note that  $\mathbb{Q}(\beta)$  has discriminant  $-1823$  and narrow class group being  $C_2$ . Also note that  $-\beta$  is a totally positive unit and  $N_{K/\mathbb{Q}}((-\beta - 1)(\beta^2 - 1)) = 7^2 \cdot 11$ . The conditions given in Theorem 4.11 give that  $H(\ell) = \mathrm{GL}_2(\mathbb{F}_\ell)$  for  $\ell \neq 7, 11, 1823$ . For these three  $\ell$ , we can use Proposition 2.12. Then using similar methods as in Section 3.4 of [Gre10] shows that the adelic Galois representation surjects onto  $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ . (See `nontriv_narrow_magma.txt` and `nontriv_narrow_sage.sws` in [CFLTL] for results of computations.)  $\square$

## 5. REMARKS ON HIGHER TORSION

Although we initially raised the problem of explicitly computing Galois representations for elliptic curves with arbitrary specified torsion data, we have primarily worked with 2-torsion in this paper. After all, it is significantly easier to produce examples of elliptic curves with 2-torsion, and to work with explicit formulas for the 2-division-polynomials. This is advantageous, for example, in verifying that the “mod 4” Galois representation is maximal (i.e.  $[K(E[4]) : K] = 16$ ), and in producing the appropriate congruence conditions in Section 3

However, many of our methods can be applied to elliptic curves with more general torsion, as we now demonstrate. We will be content to give a discussion of examples, rather than attempting to write out fully general results.

As we have observed, torsion data for  $E/K$  amounts to giving some restrictions on the “mod  $\ell^k$ ” representation

$$\rho_{E, \ell^k}(G_K) \subset \mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z}).$$

We are interested in knowing when the adelic Galois representation is maximal given such a restriction. One has to take different steps to verify that the  $\ell$ -adic Galois representation is maximal, and also account for a different abelianization map. The latter is equivalent to computing the

commutator subgroup of the desired  $\ell$ -adic image, which is reduced to a finite computation by the refinement lemmas.

Likewise, one verifies that the  $\ell$ -adic image is maximal by checking that the “mod  $\ell^k$ ” image is maximal and that the image of the Galois representation also contains the entire kernel of the reduction map  $\rho_{E,\ell^{k+1}}(G_K) \rightarrow \rho_{E,\ell^k}(G_K)$ . The first matter depends on the particular nature of the torsion data given; for instance, we consider the case of full  $\ell$ -torsion over  $K$ , in which case there is nothing to check, but if there is just one cycle of  $\ell$ -torsion points then one is looking for a “half-Borel” subgroup. We will not discuss the various cases, but instead focus on the problem of passing from finite to infinite: assuming that  $\rho_{E,\ell^k}(G_K)$  is known, how may we check that  $\rho_{E,\ell^\infty}$  is the pre-image of  $\rho_{E,\ell^k}(G_K)$  under the reduction mod  $\ell^k$  map? In the paper, we simply used the four-division polynomials for  $E$ , but this is infeasible for large  $\ell$ , so we indicate a method by analyzing Frobenius elements. Note that the Chebotarev Density Theorem certainly implies that if the  $\ell$ -adic Galois representation is maximal as desired, then a positive density of such elements must exist.

We illustrate by considering a particular example. Suppose  $E/K$  has exactly one  $\ell$ -torsion cycle for some prime  $\ell > 2$ . Suppose we want to show that  $\rho_{E,\ell^\infty}(G_K)$  is the full pre-image of the half-Borel subgroup

$$\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \subset \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}).$$

By Serre’s refinement lemma, it suffices to show that this half-Borel is in fact the mod  $\ell$  image, and to show that  $\rho_{E,\ell^2}(G_K) \supset I + 2\mathrm{Mat}_{2 \times 2}(\mathbb{Z}/\ell\mathbb{Z})$ . To address the first question, we see that the mod  $\ell$  image must be the half-Borel or the half-Cartan:

$$\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix}$$

Now, suppose  $\sigma = \mathrm{Frob}_{\mathfrak{p}}$  is found whose action on the  $\ell$ -torsion points has characteristic polynomial factoring as

$$T^2 - a_p T + p \equiv (T - 1)^2 \pmod{\ell}.$$

We would like to know whether or not  $\sigma$  is contained in the half split-Cartan subgroup. Since  $(\rho_{E,\ell}(\sigma) - I)^2 \equiv 0 \pmod{\ell}$ , if it is contained in the half split-Cartan then  $\sigma = I + \ell M$  for some  $M \in \mathrm{GL}_2(\mathbb{Z}_\ell)$ . The characteristic polynomial of  $M$  is then

$$T^2 - \frac{a_p - 2}{\ell} T + \frac{1 + p - a_p}{\ell^2}.$$

In particular,  $\ell^2 \mid 1 + p - a_p$ . So if this ever fails, we know that  $\rho_{E,\ell}$  was not contained in the split Cartan.

We now address the second question, which is a generalization of the arguments in [LT76], p. 56-57. This group  $I + 2\mathrm{Mat}_{2 \times 2}(\mathbb{Z}/\ell\mathbb{Z})$  is an abelian group isomorphic to  $(\mathbb{Z}/\ell\mathbb{Z})^4$ ; we must obtain four independent elements.

We recall the following fact: if the characteristic polynomial of a  $2 \times 2$  matrix with coefficients in  $\mathbb{Z}_\ell$  factors with *distinct* roots when considered modulo  $\ell$ , then it is diagonalizable over  $\mathbb{Z}_\ell$ . Note that it is *not* sufficient for the roots to be distinct modulo  $\ell^2$  (indeed, the polynomial may very well have four roots in  $\mathbb{Z}/\ell^2\mathbb{Z}$ ).

Step One. It is easy to obtain diagonalizable, non-scalar elements. As outlined in the paper, we may compute the characteristic polynomial of a Frobenius element at  $\sigma = \mathrm{Frob}_{\mathfrak{p}}$ :

$$T^2 - a_p T + p,$$

where  $a_p = p + 1 - \#E(\mathbb{F}_p)$ . Suppose this polynomial factors mod  $\ell^2$  as a product of two linear polynomials with *distinct* roots  $\lambda_1, \lambda_2$  such that  $\lambda_1 \not\equiv \lambda_2 \pmod{\ell}$ . Then  $\rho_{E,\ell^\infty}(\mathrm{Frob}_{\mathfrak{p}})$  may be

diagonalized over  $\mathbb{Z}_\ell$ , so it will have the form

$$\sigma \equiv \begin{pmatrix} \lambda_1 + \ell^2 x_1 & 0 \\ 0 & \lambda_2 + \ell^2 x_2 \end{pmatrix}.$$

for some  $x_1, x_2 \in \mathbb{Z}_\ell$ . Raising to the  $(\ell - 1)^{\text{st}}$  power yields

$$\sigma^{\ell-1} \equiv I + \ell \begin{pmatrix} \frac{\lambda_1^{\ell-1}-1}{\ell} & 0 \\ 0 & \frac{\lambda_2^{\ell-1}-1}{\ell} \end{pmatrix} \pmod{\ell^2}.$$

(The point is that  $\lambda_1^{\ell-1} \equiv 1 \pmod{\ell}$ , so we may legitimately do this division). As long as  $\lambda_1^{\ell-1} \not\equiv \lambda_2^{\ell-1} \pmod{\ell^2}$ , this matrix is guaranteed to be diagonal but not scalar.

*Remark.* This can only fail if the image of Galois mod  $\ell$  is trivial, since this only fails to occur when the image is contained in the normalizer of a non-split Cartan. This is impossible under our torsion assumptions. On the other hand, the image mod  $\ell$  is trivial only for small  $\ell$ , in particular  $\ell = 2$  for  $K = \mathbb{Q}$ .

Step Two. Next, suppose that a Frobenius element  $\sigma$  is found with characteristic polynomial as above, but such that  $\lambda_1^{\ell-1} \equiv \lambda_2^{\ell-1} \pmod{\ell^2}$ . Then we are guaranteed that  $\sigma^{\ell-1}$  is a scalar matrix. Adopting the basis with respect to which the matrix from the previous part is diagonal, we see that in this basis we would have *all* diagonal matrices. (The point is that we have no way of telling in which bases the diagonal matrices obtainable in (1) are diagonalizable. However, scalar matrices are scalar in *every* basis! We cannot obtain scalar matrices by the method in (1) since their eigenvalues are obviously guaranteed not to be distinct modulo  $\ell$ .)

Step Three. Now, suppose that we have produced  $\sigma \in \rho_{\ell^\infty}$  with  $\sigma = I + \ell M$ , for some  $M \in \text{GL}_2(\mathbb{Z}_\ell)$ . The characteristic polynomial of  $M$  is then

$$T^2 - \frac{a_p - 2}{\ell} T + \frac{1 + p - a_p}{\ell^2}.$$

and if this is irreducible  $\pmod{\ell}$  then we know that  $\sigma$  cannot be put into upper-triangular form in any basis. Adjusting by diagonal elements already obtained, we obtain an element of the form

$$I + \ell \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} \pmod{\ell^2}$$

where  $b, c \neq 0$ .

It remains to discuss how to produce such a sigma. Suppose  $\sigma = \text{Frob}_p$  is found with characteristic polynomial factoring as

$$T^2 - a_p T + p \equiv (T - 1)^2 \pmod{\ell}.$$

which implies that  $(\sigma - I)^2 \equiv 0 \pmod{\ell}$ . If  $\sigma$  is congruent to the identity modulo  $\ell$ , then we know that  $\sigma = I + \ell M$ . We test this in the example below by checking for full  $\ell$ -torsion in  $E(\mathbb{F}_\ell)$ . An alternative approach is to observe that  $\sigma^\ell$  *must* be congruent to the identity modulo  $\ell$ , and we can compute its characteristic polynomial from that of  $\sigma$  (We have  $\sigma^\ell = A\sigma + B$  by using the relation of the characteristic polynomial, and similarly obtain another linear relation for  $\sigma^{2\ell}$ ).

Step Four. Finally, we observe that we may conjugate any element of  $G$  by any other element. We have already shown that we have all diagonal matrices, and the previous part guarantees a matrix of the form  $I + \ell \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} \pmod{\ell^2}$ . Conjugating this by  $\begin{pmatrix} 1 & 0 \\ 0 & u \end{pmatrix}$  where  $u \neq 1$ , we obtain

$$\begin{pmatrix} 0 & u^{-1}b \\ uc & 0 \end{pmatrix}.$$

5.0.3. *Proof of Example 1.6.* To conclude, we carry out the program described above to give an example of an elliptic curve  $E/\mathbb{Q}$  and Frobenius elements satisfying the above properties. Let

$$E/\mathbb{Q}: y^2 + xy + y = x^3 - x^2 - 19353x + 958713$$

which has torsion subgroup  $\mathbb{Z}/7\mathbb{Z}$ . In this case,  $\ell = 7$ . We compute that Step 1 above is satisfied by considering the Frobenius corresponding to 61, Step 2 is satisfied by considering the Frobenius corresponding to 971. We then note that the prime  $q = 127$  is such that  $T^2 - a_q T + q \equiv (T - 1)^2 \pmod{7}$  and  $49 \nmid 1 + q - a_q$ . Moreover, the prime  $p = 19993$  is such that  $T^2 - a_p T + p \equiv (T - 1)^2 \pmod{7}$  and  $49 \mid 1 + p - a_p$ ,  $T^2 - (a_p - 2)/\ell T + (1 + p - a_p)/\ell^2$  is irreducible mod  $\ell$  and  $E(\mathbb{F}_{19993})$  has full 7-torsion. This implies that Step 3 is satisfied. (See `frob_find.txt` in [CFLTL] for computations.)  $\square$

## REFERENCES

- [Ade01] Clemens Adelmann, *The decomposition of primes in torsion point fields*, Lecture Notes in Mathematics, vol. 1761, Springer-Verlag, Berlin, 2001.
- [CFLTL] David Corwin, Tony Feng, Zane Kun Li, and Sarah Trebat-Leder, *Transcript of computations*, Available at [https://web.math.princeton.edu/~zkli/adelic\\_code/](https://web.math.princeton.edu/~zkli/adelic_code/).
- [Duk97] William Duke, *Elliptic curves with no exceptional primes*, C. R. Acad. Sci. Paris Sér. I Math. **325** (1997), no. 8, 813–818.
- [Gre10] Aaron Greicius, *Elliptic curves with surjective adelic Galois representations*, Experiment. Math. **19** (2010), no. 4, 495–507.
- [Jon10] Nathan Jones, *Almost all elliptic curves are Serre curves*, Trans. Amer. Math. Soc. **362** (2010), no. 3, 1547–1570.
- [LT76] Serge Lang and Hale Trotter, *Frobenius distributions in  $GL_2$ -extensions*, Lecture Notes in Mathematics, Vol. 504, Springer-Verlag, Berlin, 1976, Distribution of Frobenius automorphisms in  $GL_2$ -extensions of the rational numbers.
- [Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d’ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.
- [Ser98] ———, *Abelian  $l$ -adic representations and elliptic curves*, Research Notes in Mathematics, vol. 7, A K Peters Ltd., Wellesley, MA, 1998, With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.
- [Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.
- [Zyw10a] David Zywina, *Elliptic curves with maximal Galois action on their torsion points*, Bull. Lond. Math. Soc. **42** (2010), no. 5, 811–826.
- [Zyw10b] ———, *Hilbert’s irreducibility theorem and the larger sieve*, Preprint (2010), arXiv:1011.6465v1.

DEPARTMENT OF MATHEMATICS, PRINCETON UNIVERSITY, PRINCETON, NEW JERSEY 08544  
 E-mail address: dcorwin@math.princeton.edu

479 QUINCY MAIL CENTER, 58 PLYMPTON STREET, CAMBRIDGE, MA 02138  
 E-mail address: tfeng@college.harvard.edu

DEPARTMENT OF MATHEMATICS, PRINCETON UNIVERSITY, PRINCETON, NEW JERSEY 08544  
 E-mail address: zkli@math.princeton.edu

DEPARTMENT OF MATHEMATICS, PRINCETON UNIVERSITY, PRINCETON, NEW JERSEY 08544  
 E-mail address: strebat@math.princeton.edu